LE BLANCHIMENT DE LA MONNAIE ÉLECTRONIQUE
Analyse de l'environnement

Justice Canada

Solliciteur général Canada

Octobre 1998

« Les administrations devraient examiner les menaces que représentent les nouvelles technologies telles que les cartes intelligentes et la banque électronique lorsqu'elles sont utilisées pour blanchir de l'argent et prendre les mesures nécessaires pour prévenir l'emploi de ces technologies à des fins malhonnêtes. »
(Groupe d'action financière international, 1996)

La présente analyse de l'environnement vise à stimuler la réflexion sur les nouvelles questions qui se posent en matière de justice pénale. Elle ne représente cependant pas la politique du ministère du Solliciteur général du Canada ou du gouvernement du Canada, ni celle d'autres ministères ou organismes fédéraux.

TABLE DES MATIÈRES

PREFACE ii

RÉSUMÉ iii

1.0 LE BLANCHIMENT DE L'ARGENT 1
- **1.1 Qu'est-ce que le blanchiment de l'argent?** 1
- **1.2 Les conséquences du blanchiment de l'argent** 2
- **1.3 Stratégies et initiatives** 2

2.0 LA MONNAIE ÉLECTRONIQUE 5
- **2.1 Qu'est-ce que la monnaie électronique?** 5
- **2.2 L'étendue de la monnaie électronique** 6
- **2.3 Le risque de blanchiment d'argent électronique** 8

3.0 DÉFIS EN MATIÈRE DE JUSTICE PÉNALE 11
- **3.1 Questions touchant la législation et la réglementation** 11
- **3.2 Questions relatives à la police et à l'application de la loi** 12

4.0 COOPÉRATION INTERNATIONALE 15

5.0 CONCLUSION 19

BIBLIOGRAPHIE 21

ANNEXES

Annexe I : Le fonctionnement des systèmes de monnaie électronique 31
Annexe II : Cryptographie et commerce électronique 33
Annexe III : Caractéristiques des systèmes de paiement 35
Annexe IV : Aperçu des politiques sur la monnaie électronique établies par les pays du G-10 37
Annexe V : Recommandations du GAFI 45

PREFACE

Cette analyse environnementale s'inscrit dans un partenariat continu établi entre le ministère de la Justice du Canada et le Solliciteur général du Canada. *Le blanchiment de la monnaie électronique* a été écrit par Jasmine Brown et Austin Lawrence, du ministère de la Justice, et Darryl Sitka et Raffaele Fasiolo du Solliciteur général du Canada.

Cette analyse définit d'abord ce qu'est l'argent électronique et examine ses effets avant de préciser la portée de ce concept et les possibilités relatives au blanchissage électronique de l'argent. Elle étudie les défis du système canadien de justice pénale et évalue enfin l'importance de la coopération internationale.

RÉSUMÉ

Le présent rapport a été produit par les ministères du Solliciteur général et de la Justice du Canada.

Dans les nouveaux systèmes financiers, la valeur économique des échanges est représentée sous une forme électronique. Ces échanges électroniques sont possibles grâce à de nouvelles technologies telles que les cartes intelligentes et Internet. La monnaie électronique est censée remplir la même fonction que la monnaie-papier, mais sans les risques, les inconvénients et les coûts reliés à la manipulation, à la gestion et à la protection de l'argent liquide.

Le développement fulgurant de la technologie de la monnaie électronique engendre divers problèmes dont le blanchiment d'argent. Tout crime qui rapporte des sommes importantes – extorsion, trafic des stupéfiants, trafic d'armes et certains types de criminalité des cols blancs – peut donner lieu à des tentatives de blanchiment d'argent.

La monnaie électronique peut présenter de l'intérêt pour les blanchisseurs d'argent pour deux principales raisons : les opérations électroniques peuvent être effectuées de manière à ne pas laisser de *traces* et elles offrent une *mobilité incroyable*. Il est facile d'effectuer des opérations électroniques anonymes qui ne permettront pas d'établir une piste de vérification traditionnelle. La technologie de la monnaie électronique permet aussi d'effectuer instantanément des virements de fonds d'un pays à un autre sans aucune restriction imposée par les autorités des pays visés.

Dans ce contexte, il pourra être nécessaire, pour prévenir et dépister le blanchiment d'argent électronique et arrêter les auteurs de ce type de crime, de mettre en oeuvre de nouvelles mesures législatives et réglementaires, de recourir à de nouvelles techniques en matière d'enquêtes et d'application de la loi et, ce qui est plus important encore, d'accroître la coopération internationale. Des mesures devraient probablement être prises dans plusieurs champs d'activité :

- outils plus efficaces mis à la disposition des organismes d'application de la loi;
- formation, tant pour les membres des organismes d'application de la loi que dans le secteur financier, notamment au sein des organismes de réglementation de ce secteur;
- échange et enregistrement de renseignements, au Canada et à l'échelle internationale;
- modification des lois sur le secret bancaire, de manière à faire obstacle au blanchiment d'argent mais non aux opérations légitimes.

1.0 LE BLANCHIMENT DE L'ARGENT

Pour pouvoir saisir toutes les répercussions que peuvent avoir les technologies de la monnaie électronique sur le blanchiment de l'argent, il faut d'abord comprendre comment fonctionne le blanchiment de l'argent.

1.1 Qu'est-ce que le blanchiment de l'argent?

Le blanchiment d'argent consiste à recycler ou à transférer des biens, c'est-à-dire des produits de la criminalité, dans le but de cacher aux autorités gouvernementales leur nature et leur origine illicites.

Toute activité criminelle qui génère des profits importants – extorsion, trafic des stupéfiants, trafic d'armes et certains types de criminalité des cols blancs – peut donner lieu au blanchiment d'argent.

De quelle façon l'argent est-il blanchi? En général, l'argent est transféré d'un pays à un autre (par des moyens physiques ou électroniques) et son origine est camouflée au moyen de transactions financières complexes. D'après le Groupe d'action financière international (GAFI), les estimations des sommes blanchies chaque année dans le monde, uniquement dans le secteur du trafic des drogues, se situent entre 300 milliards et 500 milliards de dollars US. Si l'on inclut l'argent tiré des crimes économiques et d'autres formes de criminalité non associées à la drogue, ces chiffres pourraient doubler (Porteous, 1998).

Le blanchiment de l'argent représente pour notre économie une perte de plusieurs milliards de dollars.

On a estimé la taille du marché des drogues illicites au Canada entre 7 et 10 milliards de dollars. D'après les experts, de 50 à 70% des revenues tirés de la vente des drogues sont disponibles pour être blanchis et réinvestis. Si l'on suppose en outre, comme certains l'ont soutenu, que de 50 à 70 % des fonds blanchis au Canada proviennent du commerce de la drogue, on peut dire que chaque année, au Canada, entre 5 et 14 milliards de dollars d'argent illicite est blanchi (Porteous, 1998)

Le blanchiment d'argent qui n'est pas relié au trafic des stupéfiants se rapporte généralement à des activités reliées au crime organisé, par exemple la contrebande de l'alcool, des produits du tabac et des armes à feu, la pornographie, l'immigration clandestine (réseaux de passeurs), les jeux de hasard illégaux ainsi que la prostitution.

L'évasion fiscale à grande échelle dans l'économie souterraine mène également au blanchiment d'argent, car les contrevenants cherchent des moyens de cacher leurs revenus au Canada ou de les transférer à l'étranger.

Les méthodes traditionnelles de blanchiment d'argent comprennent le recours à des sociétés fantômes, aux pays refuges et à des entreprises dont les recettes sont uniquement en argent

liquide et l'utilisation abusive de certains services financiers offerts par les banques et autres institutions de dépôt. Les nouveaux marchés financiers (par exemple, les secteurs des valeurs mobilières et de l'assurance et les bureaux de change) attirent aussi de plus en plus les blanchisseurs de grosses sommes d'argent.

Une quantité importante de devises fortes (sous forme d'argent liquide, d'obligations ou de certificats d'actions) franchit la frontière canado-américaine par l'entremise de passeurs ou à l'intérieur de chargements. Les transferts électroniques de fonds (virements télégraphiques) sont de plus en plus fréquents, et l'utilisation d'Internet préoccupe de plus en plus les autorités.

1.2 Les conséquences du blanchiment de l'argent

Le blanchiment de l'argent est lourd de conséquences :

- **Le crime devient payant.** Le blanchiment de l'argent permet aux trafiquants de drogue, aux contrebandiers et autres criminels d'étendre leurs opérations, d'où une augmentation du coût de l'application de la loi et des soins de santé (p. ex., traitement des toxicomanes).

- Le blanchiment de l'argent peut avoir pour effet **d'ébranler les milieux financiers** en raison de l'ampleur des sommes en cause. Le risque de corruption augmente à mesure que les montants d'argent en circulation obtenus par des moyens illégaux s'accroissent.

- **Les recettes fiscales diminuent**, d'où les préjudices causés indirectement aux contribuables honnêtes et la diminution des possibilités d'emploi dans les entreprises légitimes.

- Du fait qu'on croit qu'il est facile d'entrer au Canada, notre pays **attire des éléments indésirables**, il s'ensuit une détérioration de notre qualité de vie et la sécurité nationale se trouve menacée.

1.3 Stratégies et initiatives

> Le blanchiment de l'argent touche tous les Canadiens, dans les rues et dans les collectivités.

Des mesures sont mises en oeuvre au Canada et ailleurs dans le monde pour lutter contre le blanchiment de l'argent. Par exemple, le renforcement du leadership à l'échelle nationale, l'adoption de nouvelles lois, de nouveaux règlements et de nouvelles politiques financières, une coopération internationale et des contrôles à la frontière. Nous exposerons dans les paragraphes qui suivent certaines des stratégies et initiatives clés actuelles.

Le Canada a mis en application **de nouvelles lois et de nouveaux règlements** pour lutter contre le blanchiment de l'argent. Par exemple, des modifications ont été apportées au *Code criminel* en

vue de criminaliser le blanchiment de l'argent et on a adopté des dispositions prévoyant l'obligation de tenir des registres en vue de faciliter les enquêtes et les poursuites.

Les modifications apportées récemment au *Code criminel* dans le cadre du projet de loi C-95 donnent à la police, aux procureurs de la Couronne et aux tribunaux une série de nouveaux pouvoirs dans le contexte de la lutte contre le crime organisé. De plus, on envisage d'apporter des modifications législatives visant la création d'un régime de rapports obligatoires sur les transactions suspectes et le contrôle des mouvements transfrontaliers de devises.

Pour combattre le transfert de fonds illicites entre le Canada et les autres pays, les agents des douanes pourraient se voir confier des pouvoirs accrus grâce auxquels ils pourraient procéder à des fouilles et détenir des devises et autres instruments financiers suspects. Bien que les Douanes soient habilitées à effectuer des fouilles et à détenir des marchandises suspectes, les devises ne sont pas incluses dans la définition de « marchandises ». On envisage de modifier la loi en vue de corriger cette situation.

Le Canada pourrait également envisager de créer un **organisme central** chargé de surveiller la plupart des activités menées dans le cadre des initiatives améliorées en matière de lutte contre le blanchiment de l'argent. Actuellement, un comité national de coordination et cinq comités régionaux de coordination composés de représentants de la police et d'autres organismes tiennent régulièrement des réunions en vue de définir les meilleures pratiques et d'échanger des renseignements, de sorte qu'une approche multidisciplinaire est adoptée pour lutter contre le crime organisé.

Le gouvernement canadien travaille à l'élaboration de lois et de contrôles plus sévères pour lutter contre le blanchiment de l'argent.

Le Canada **travaille en étroite collaboration avec d'autres pays** pour améliorer l'échange de renseignements et établir des stratégies visant les paradis fiscaux et les juridictions fiscales des pays où il existe une loi sur le secret bancaire. Ce travail est effectué par des organismes internationaux tels que l'Organisation de coopération et de développement économiques et la Pacific Association of Tax Administrators dans le cadre de discussions bilatérales avec les pays signataires des conventions et d'échanges de renseignements.

Le Canada participe aussi activement aux travaux du Groupe d'action financière international établi par le G-7 dans le but de lutter contre le blanchiment de l'argent, du Groupe de travail P-8 sur le crime organisé transnational, de la Commission interaméricaine de lutte contre l'abus des drogues, du forum sur la criminalité transfrontalière et d'autres organisations qui se consacrent à la lutte contre le crime organisé de nature essentiellement financière. Des discussions ont également lieu au sein de la Commission pour la prévention du crime et la justice pénale des Nations Unies en vue de la création d'un mécanisme international de lutte contre le crime organisé transnational.

Des protocoles d'entente et des traités d'entraide juridique pourraient être conclus pour assurer des échanges de renseignements efficaces et la conclusion d'ententes équitables sur le partage des biens.

Il existe déjà des mécanismes pour lutter contre le blanchiment de l'argent par des méthodes traditionnelles, mais de nouvelles approches devraient être adoptées pour faire face à la menace particulière que représente le blanchiment de l'argent *électronique*.

2.0 LA MONNAIE ÉLECTRONIQUE

2.1 Qu'est-ce que la monnaie électronique?

Étant donné sa structure décentralisée, la monnaie électronique est susceptible de transformer la structure économique de la même façon que les ordinateurs personnels ont transformé la structure de la gestion et des communications. ***(Birch et McEvoy, 1996)***

Les nouveaux systèmes financiers permettent de représenter la valeur économique sous une forme numérique à l'aide de dispositifs électroniques. La monnaie électronique peut être échangée contre des biens ou des services à l'aide de « cartes intelligentes » ou sur Internet.

Contrairement aux porte-monnaie électroniques, la monnaie électronique peut être transmise immédiatement lors d'une transaction en ligne entre deux parties, sans intermédiaire (p. ex., DigiCash Inc.).

La monnaie électronique est censée en définitive remplir la même fonction que la monnaie-papier, mais sans les risques, les inconvénients et les coûts associés à la manipulation, à la gestion et à la protection de la monnaie traditionnelle.

(Pour de plus amples renseignements sur la façon dont la monnaie électronique fonctionne, consulter l'annexe I.)

Une très grande variété de systèmes de paiement électronique sont mis au point actuellement dans de nombreux pays. Étant donné que ces systèmes évoluent sans cesse, pour des raisons pratiques, nous ne décrirons pas ici leur fonctionnement.

La monnaie électronique transformera la structure de notre économie.

Les lecteurs qui désirent en savoir davantage sur le sujet pourront consulter certains des nombreux ouvrages énumérés dans la bibliographie. Dans la présente section, nous nous contenterons de définir la nature de la monnaie électronique et son ampleur et d'indiquer le rôle qu'elle pourrait jouer dans le blanchiment de l'argent.

Les systèmes de paiement ont évolué au même rythme que la technologie. La monnaie électronique représente la méthode d'échange la plus récente. Les gouvernements doivent être prêts à intervenir face aux nouvelles possibilités offertes par cette monnaie et à la menace qu'elle représente.

Les opérations électroniques ne constituent nullement une toute nouvelle technologie. Les banques et autres institutions financières utilisent les ordinateurs pour les transferts entre établissements depuis déjà un certain temps.

Aux États-Unis, 90 % de toutes les opérations sont effectuées au moyen de deux systèmes, le Fedwire et le Clearing House Interbank Payments System (ou CHIPS), si on considère le *volume*

des dollars échangés. Ces systèmes sont surtout utilisés par d'importantes institutions financières.

Par contre, si on compte le nombre d'opérations, 90 % sont encore effectuées en argent ou par chèque. Il s'agit d'opérations à petite échelle effectuées par des particuliers. Ces statistiques sont valables aussi pour le Canada.

Grâce aux progrès réalisés dans trois secteurs technologiques, la monnaie électronique s'est de plus en plus répandue et elle est devenue viable sur le plan économique, d'où l'intérêt pour cette monnaie. Ces progrès sont les suivants :

- les communications en réseau, fiables et rapides, permettent d'effectuer des opérations à un coût peu élevé;
- les progrès de l'ordinatique ont permis la production en série de cartes à puce;
- l'utilisation de la cryptographie s'est généralisée et a contribué à assurer efficacement la protection des renseignements personnels et à prévenir la fraude. (Voir l'annexe II pour de plus amples renseignements sur la cryptographie et le commerce électronique.)

Ce qu'il y a de révolutionnaire dans les systèmes de monnaie électronique qui sont mis au point actuellement, c'est qu'ils sont conçus pour imiter l'argent traditionnel. Sur un plan stratégique, ces systèmes pourront donc occuper une place importante dans le marché des petites opérations, qui représentent la majeure partie de toutes les opérations effectuées. La monnaie électronique aura plus de répercussions sur la société qu'en ont eu les progrès du commerce électronique dans le passé, car elle changera la vie du citoyen moyen et celui-ci contribuera également à faire évoluer ce mode de paiement. (Voir l'annexe III pour une comparaison entre les systèmes de paiement actuels et les cyberpaiements.)

2.2 L'étendue de la monnaie électronique

La valeur réelle des opérations commerciales effectuées sur Internet n'est pas très élevée actuellement. Selon une estimation non officielle, les opérations effectuées annuellement sur Internet ne représentent actuellement qu'environ 100 à 200 millions de dollars. (Conférence du Département américain des finances, 1996) Cependant, certains prévoient que cette valeur (qui n'inclut pas les opérations au moyen des cartes intelligentes) montera en flèche et représentera environ 10 milliards de dollars d'ici l'an 2000.

Bien que le commerce sur Internet n'ait pas encore une grande ampleur, la technologie de la monnaie électronique est au point et ce type de commerce pourrait prendre de l'expansion rapidement. Selon le magazine *Smart Cards*, une publication dans le secteur du commerce, d'ici l'an 2001, le volume des opérations commerciales effectuées à l'aide des cartes intelligentes pourrait représenter plus de 100 milliards de dollars. (Cherneff *et coll.*, 1996)

On a déjà commencé à produire le matériel informatique qui permettra une pénétration importante du marché des achats à domicile à l'aide de la monnaie électronique. Par exemple,

Microsoft, Hewlett-Packard et Gemplus produisent déjà des claviers d'ordinateurs personnels capables de lire les cartes intelligentes. AT&T prévoit convertir ses téléphones publics pour qu'ils puissent fonctionner au moyen de cartes intelligentes. Mondex et Digi-Cash mettent à l'essai des cartes intelligentes dans plusieurs pays dans le cadre de projets pilotes. Même le gouvernement américain a l'intention de mettre en place des systèmes basés sur l'utilisation de la monnaie électronique. Il étudie la possibilité de procéder à des transferts électroniques pour le versement des prestations d'ici 1999.

En définitive, ce seront les consommateurs et les entreprises qui décideront, par leur degré d'acceptation de la monnaie électronique, de l'ampleur que prendra l'utilisation de cette monnaie. La monnaie électronique présente plusieurs avantages pour les consommateurs. Par exemple :

- des opérations plus rapides et plus efficientes;
- moins d'argent de poche nécessaire;
- fidélité et plans avantageux pour les utilisateurs fréquents;
- tenue automatique de registres financiers personnels;
- anonymat possible des opérations financières;
- protection possible contre les vols;
- accès au commerce électronique;
- services et instruments bancaires plus personnalisés.

Les avantages possibles de la monnaie électronique pour les entreprises sont nombreux. Par exemple :

- opérations instantanées;
- économies substantielles réalisées grâce à une moins grande manipulation de la monnaie;
- collecte plus facile de renseignements sur les consommateurs aux fins du marketing;
- promotion des opérations bancaires gratuites.

Le temps et la distance ont toujours été les deux plus importantes contraintes dans le commerce. Ces deux contraintes disparaissent grâce aux systèmes de monnaie électronique. Ces systèmes contribueront sûrement à la mondialisation des marchés.

Cependant, plusieurs obstacles risquent d'interrompre ou de ralentir la progression de l'utilisation de la monnaie électronique s'ils ne sont pas éliminés. Par exemple :

- le coût de l'installation de l'infrastructure technologique peut être important;

- les systèmes de monnaie électronique devront être compatibles avec les modes de paiement actuels et pouvoir y être intégrés;

- le coût d'utilisation du système devra demeurer inférieur au coût d'utilisation des systèmes de paiement actuels;

- le risque de perdre une carte et la valeur économique qu'elle représente pourrait représenter un inconvénient pour certains consommateurs;

- comme la sécurité est un aspect important pour les utilisateurs, les systèmes de monnaie électronique devraient posséder les caractéristiques suivantes : convertibilité, possibilité d'obtenir des reçus et niveau élevé de sécurité;

- la protection des renseignements personnels constituera aussi un aspect important.

On trouvera probablement des solutions à tous ces problèmes. Tout compte fait, il semble probable que la monnaie électronique occupera une place importante dans notre vie quotidienne dans un proche avenir.

2.3 Le risque de blanchiment d'argent électronique

L'utilisation abusive de la monnaie électronique par les blanchisseurs d'argent constitue une menace importante.

Que représente la monnaie électronique pour le blanchisseur d'argent?

On croit pour l'instant que le risque de blanchiment de l'argent électronique est négligeable.

> Jusqu'ici, les pays du G-10 n'ont rien noté qui puisse indiquer qu'il y ait des activités de blanchiment d'argent en rapport avec la technologie de la monnaie électronique. Si cette technologie était utilisée sur une grande échelle, il est concevable que les criminels puissent chercher à en tirer parti pour le transfert de fonds illicites. (Groupe des dix, 1997)

En effet, les criminels sont toujours à l'affût d'un nouveau type de détergent pour mieux lessiver leur argent. (Bortner, 1996) Jusqu'ici, ils n'ont pas mis de temps à tirer profit de chaque nouvelle méthode de transfert financier. Dans les années 80 et 90, les virements télégraphiques sont devenus populaires pour le transfert de fonds tant à des fins légitimes qu'à des fins illégitimes. D'ici l'an 2000, le même phénomène pourrait se produire dans le cas de la monnaie électronique

Les blanchisseurs d'argent pourraient à l'avenir faire une utilisation abusive de la monnaie électronique et cela pourrait constituer un problème grave. Les blanchisseurs d'argent seront attirés par cette monnaie pour deux raisons :

- les opérations peuvent ne pas laisser de traces;
- elles offrent une mobilité incroyable.

L'utilisation de la monnaie électronique pourrait présenter deux avantages pour les membres du crime organisé : elle ne laisse pas de traces et elle offre une grande mobilité.

Possibilité de ne pas laisser de traces

Avec l'introduction de la monnaie électronique, très peu d'opérations seront effectuées en personne. Il sera donc plus difficile de « connaître les clients ».

Les systèmes de monnaie électronique permettront aux parties d'effectuer des opérations entre eux sans passer par les institutions financières réglementées. Par conséquent, la piste de vérification traditionnelle ne pourra pas toujours être suivie.

Mobilité

Hypothétiquement, la monnaie électronique pourrait venir de n'importe quel pays et être envoyée partout dans le monde. Il serait donc possible d'effectuer des virements instantanément au moyen d'un réseau qui, en fait, ne serait pas réglementé.

Pour illustrer le problème que pose l'utilisation de la monnaie électronique, il est nécessaire de distinguer les trois étapes de base du blanchiment d'argent — le placement de l'argent, les virements successifs et l'intégration, et de comparer les systèmes de blanchiment d'argent traditionnels avec les cybersystèmes.

La première étape du blanchiment d'argent est l'écoulement de l'argent liquide (le *placement*). L'argent peut être déposé dans une banque ou une autre institution financière au pays. Il peut aussi être introduit clandestinement dans d'autres pays en vue d'y être déposé dans des comptes. Il peut aussi être utilisé pour acheter des biens de grande valeur, comme des oeuvres d'art, des avions, des métaux précieux ou des pierres précieuses qui peuvent être revendus et payés par chèque ou par virement bancaire.

Dans le cas du blanchiment de l'argent électronique, des sommes d'argent peuvent être déposées dans une institution financière non réglementée. Le placement peut facilement se faire en achetant, par exemple, des devises étrangères ou des biens au moyen d'une carte intelligente ou d'un ordinateur personnel. On aura recours à un cryptage complexe pour assurer l'anonymat des opérations.

La deuxième étape, la *technique des virements successifs*, consiste à effectuer des virements successifs complexes dans le but d'établir une distance entre les produits illicites et leur source et de brouiller la piste de vérification. Pour arriver à leurs fins, les blanchisseurs font des virements télégraphiques de l'argent liquide qui a été déposé, convertissent l'argent déposé en instruments financiers (p. ex., des obligations, des actions ou des chèques de voyage), revendent les biens de grande valeur ou les instruments financiers ou investissent dans l'immobilier et dans des entreprises légitimes, surtout dans les secteurs des loisirs et du tourisme. Pour effectuer une série de virements, on se sert beaucoup de sociétés fantômes, qui sont généralement enregistrées dans des paradis fiscaux. Ces sociétés, dont les administrateurs sont souvent des avocats qui agissent à titre de propriétaires apparents, cachent l'identité des véritables propriétaires. Les propriétaires réels bénéficient de lois sur le secret bancaire et du privilège du secret professionnel de l'avocat.

Dans les systèmes de monnaie électronique, les virements successifs peuvent être effectués au moyen d'un ordinateur personnel. Ces opérations ne laissent généralement aucune piste de vérification. De plus, les systèmes de monnaie électronique permettent des virements de fonds instantanés, dans un cadre où il n'y a pas de frontières.

La dernière étape, *l'intégration,* consiste à prendre des mesures pour s'assurer que les produits de la criminalité paraissent légitimes. Diverses techniques traditionnelles sont utilisées, notamment le recours à des sociétés-écrans qui « prêtent » aux blanchisseurs des sommes d'argent qu'ils y ont placées, ou encore l'utilisation de fonds déposés dans des institutions financières à l'étranger pour garantir des prêts au pays. Une autre technique courante est la surfacturation, ou encore la production de fausses factures, pour des biens vendus, ou soi-disant vendus, dans d'autres pays.

Dans le blanchiment de l'argent électronique, le criminel peut réaliser l'intégration des produits de la criminalité en se servant d'un ordinateur personnel pour faire des placements ou acheter des biens sans recourir aux services d'une institution financière.

Bref, les blanchisseurs d'argent seront tentés d'utiliser la monnaie électronique parce qu'elle ne laisse pas de traces et qu'elle offre une grande mobilité.

3.0 DÉFIS EN MATIÈRE DE JUSTICE PÉNALE

3.1 Questions touchant la législation et la réglementation

Le blanchiment de l'argent n'est qu'un des nombreux problèmes complexes auxquels doit s'attaquer le législateur depuis l'introduction de la monnaie électronique. Comme le blanchiment de l'argent électronique est une forme particulière de crime économique assisté par ordinateur, il relève de plusieurs branches du droit : droit commercial, protection de la vie privée, droit de l'informatique, droit bancaire, droit de la propriété intellectuelle et droit criminel. Les répercussions exactes de cette nouvelle technologie sur le plan juridique restent à déterminer.

Les lois et règlements actuels exigent que les entreprises et les consommateurs fournissent des renseignements pour que le gouvernement puisse lutter contre certains types de crimes économiques. Pour ce qui est des systèmes de paiement électronique, il n'y a rien de bien défini sur le plan de l'application de la loi.

Les lois et règlements actuels pourraient devoir être modifiés.

En général, les organismes de réglementation considèrent qu'il faut laisser les forces du marché s'exercer. Étant donné le rythme effréné de l'innovation technologique, les autorités ont hésité jusqu'ici à établir de nouvelles dispositions régissant la monnaie électronique tant qu'elles ne seront pas fixées sur les formes et les usages de ce type de monnaie.

Certains pays ont néanmoins déjà commencé à modifier leurs lois de manière à y intégrer des dispositions portant sur l'utilisation de la monnaie électronique. L'Europe est plus avancée que l'Amérique du Nord à cet égard, car elle a déjà commencé à réglementer ce secteur et à établir un contrôle centralisé. (Voir l'annexe IV pour un aperçu des politiques sur la monnaie électronique établies par les pays du G-10.)

- Certains États américains ont commencé à étendre l'application des règlements relatifs à la transmission de l'argent aux fournisseurs de monnaie électronique.

- Le gouvernement américain a aussi modifié les classifications de sa loi intitulée *Electronic Fund Transfer Act* de manière à distinguer les opérations en ligne et les opérations hors ligne des systèmes de monnaie électronique.

- L'Allemagne envisage de modifier sa loi sur les banques en vue d'inclure les transferts de monnaie électronique dans le répertoire des opérations bancaires, établissant ainsi un principe de base selon lequel seules les banques seraient autorisées à appliquer des méthodes de paiement électronique.

Le Canada a décidé d'attendre et de surveiller l'évolution de la situation avant d'adopter des dispositions sur l'utilisation de la monnaie électronique. Il concentre actuellement ses efforts sur

des communications avec les entreprises qui s'intéressent à la monnaie électronique et avec d'autres gouvernements.

Au Canada, les principales lois qui pourraient comporter des dispositions sur le blanchiment de l'argent électronique sont :

- la *Loi sur le recyclage des produits de la criminalité* et le Règlement connexe;
- la *Loi sur les banques* et le Règlement connexe;
- le chapitre C-46 du *Code criminel* (en particulier le paragraphe 462.31 intitulé « Recyclage des produits de la criminalité »).

En bref, les gouvernements ont concentré leurs efforts sur la recherche, l'établissement de réseaux et la surveillance des activités dans le nouveau secteur que représente la monnaie électronique.

3.2 Questions relatives à la police et à l'application de la loi

À mesure que l'utilisation des systèmes de monnaie électronique prendra de l'ampleur, les gouvernements devront décider des mesures à prendre au chapitre de la législation et de la réglementation pour lutter contre le blanchiment d'argent et les autres crimes économiques commis à l'aide de ces systèmes. La police pourrait devoir mettre au point de nouvelles techniques pour dépister les opérations en ligne effectuées à des fins criminelles. Toutefois, il est probable que lois et règlements seront toujours en retard par rapport aux progrès technologiques et les criminels continueront à tirer profit de la technologie et essaieront de conserver une longueur d'avance sur la loi.

Le risque que les membres du crime organisé, les blanchisseurs d'argent et autres criminels du secteur financier fassent un usage illégitime des systèmes de monnaie électronique pourrait être important. Étant donné que la monnaie électronique pourrait être utilisée pour effectuer des opérations qui ne laissent pas de traces et que cette monnaie offre une mobilité sans précédent – rapidité des transferts et absence de frontières – elle pourrait engendrer des défis nouveaux sur le plan de l'application de la loi.

- Comme les nouveaux systèmes de paiement ne comporteront pas de supports papier et que les utilisateurs seront anonymes, les autorités ne pourront se servir autant qu'avant des techniques traditionnelles telles que les analyses de documents financiers et la surveillance des individus soupçonnés de crimes économiques.

- Sans piste de vérification, il sera beaucoup plus difficile pour les organismes d'application de la loi de dépister et d'empêcher les activités illicites effectuées au moyen de la monnaie électronique et de faire enquête sur ces activités.

- Étant donné que les transactions sont instantanées, il est plus difficile de les dépister, d'exercer une surveillance et d'appréhender des individus. Par exemple, une fois qu'un crédit à codification numérique a été établi, il peut être utilisé pour n'importe quelle opération. À l'exception des factures de téléphone, il n'y aura aucun registre des opérations effectuées, qui seront en général protégées grâce à un système de cryptage à clé. Et si un numéro 1-900 a été utilisé pour camoufler l'appel, celui-ci ne paraîtra pas sur la facture de téléphone. Par conséquent, les enquêtes coûteront plus cher et seront plus difficiles à mener.

La police devra peut-être mettre au point de nouvelles techniques de dépistage, de surveillance et d'enquête.

- Si les opérations ne sont pas effectuées à l'intérieur de limites géographiques précises, la question de la juridiction devient beaucoup plus complexe. Si on ne sait pas *où* l'activité criminelle a été commise, comment savoir *qui* devrait être chargé de mener l'enquête ou d'intenter des poursuites.

Il faudra nécessairement évaluer la situation en fonction des caractéristiques des systèmes de paiement électronique et des différents types de monnaie électronique. Par exemple, les systèmes actuels de cartes intelligentes comme Mondex laissent des pistes de vérification et limitent la valeur maximale des cartes. Des rapports produits par les autorités des pays où ces cartes sont utilisées indiquent que les criminels s'intéressent peu à ces cartes (Conférence du Département américain des finances, 1996). Cependant, les organismes d'application de la loi sont préoccupés par le fait que, dans l'avenir, les systèmes de monnaie électronique pourraient permettre à leurs utilisateurs d'effectuer, sans laisser de piste de vérification, des opérations anonymes et instantanées à l'étranger. Ils devront peut-être mettre au point de nouvelles techniques de dépistage, de surveillance et d'enquête afin d'empêcher les blanchisseurs d'argent de se servir des systèmes de paiement électronique pour leurs activités criminelles.

4.0 COOPÉRATION INTERNATIONALE

L'arme la plus importante pour lutter contre le blanchiment de l'argent électronique est la coopération internationale. Étant donné que la monnaie électronique n'est pas limitée par les frontières, dans le domaine de la lutte contre le blanchiment d'argent, les lois, les règlements, les techniques d'enquête et les mécanismes d'application de la loi ne constituent que le maillon le plus faible de la chaîne internationale.

Depuis environ 15 ans, les gouvernements unissent leurs efforts dans la lutte contre le blanchiment de l'argent. Les principales ententes internationales sur le blanchiment de l'argent ont été établies lors de la Convention de Vienne de 1988 des Nations Unies et de la Convention de 1990 du Conseil de l'Europe.

Le Comité de Bâle des règles et pratiques de contrôle des opérations bancaires, l'Union européenne et l'Organisation internationale des commissions de valeurs ont examiné le rôle des institutions financières dans la prévention et le dépistage du blanchiment d'argent. D'importants organismes internationaux, dont le Groupe d'action financière international (GAFI) et le G7/P8 (Groupe de Lyon), essaient de guider les organismes d'application de la loi chargés de prévenir et de dépister le blanchiment d'argent et d'arrêter les auteurs de ce type de crime.

Les techniques d'enquête et les mécanismes d'application de la loi ne constituent que le maillon le plus faible de la chaîne internationale.

Le GAFI est le principal organisme international qui effectue un travail continu et approfondi en vue de définir des politiques et de promouvoir des contre-mesures à l'égard du blanchiment de l'argent. Le Canada est un membre actif de ce Groupe de travail. Le GAFI a adopté 40 recommandations détaillées sur des sujets tels que l'identification des clients, l'établissement de normes minimales sur la tenue de registres, la coopération entre les banques, le travail des organismes de surveillance et d'application de la loi ainsi que la production de rapports sur les opérations suspectes. (Voir l'annexe V pour la liste complète des recommandations.)

Le Groupe de Lyon concentre ses efforts sur les mécanismes légaux pouvant être utilisés pour lutter contre les crimes économiques, et en particulier le blanchiment de l'argent. Un sous-groupe composé d'experts en haute technologie a étudié des moyens de repérer et d'identifier les escrocs informatiques qui se livrent à des activités criminelles au moyen de réseaux informatiques sans fil et de recueillir et échanger des éléments de preuve, notamment lorsqu'il faut effectuer des recherches à l'extérieur des frontières.

Les points saillants de certaines des recommandations les plus pertinentes sont présentés ci-dessous.

Mesures internes

- S'assurer qu'il existe des mécanismes d'entraide juridique appropriés, notamment des traités, de sorte que les institutions financières soient tenues de produire des registres et autres documents, sur demande, ainsi que d'autres types d'assistance.

- Donner aux organismes d'application de la loi les pouvoirs nécessaires pour leur permettre de reconnaître, de bloquer ou de confisquer les produits de la criminalité ou de découvrir les méthodes utilisées pour la perpétration des crimes économiques.

- Accroître les exigences relatives à l'identification des clients et à la tenue de registres en vue de faciliter le dépistage et la déclaration des opérations suspectes, la découverte des blanchisseurs d'argent et les poursuites à leur endroit.

- Adopter des lois grâce auxquelles il sera possible de tenir les personnes morales criminellement responsables dans certaines situations.

- Encourager tous les pays à considérer les crimes économiques graves comme des infractions pouvant entraîner l'extradition.

Formation et sensibilisation

- Établir des programmes internationaux de formation pour aider les gouvernements à mettre au point des opérations efficaces permettant de faire appliquer les dispositions sur les crimes économiques et pour encourager la coopération entre les organismes d'application de la loi.

- Donner une formation appropriée dans le secteur financier pour qu'il soit possible de définir les faiblesses du système et de trouver des solutions.

- Donner une formation aux organismes de réglementation du secteur des finances et à leurs examinateurs afin de les aider à mieux dépister les crimes économiques. Établir des programmes de formation au sein des institutions financières afin d'aider les employés à mieux dépister et prévenir les crimes économiques et à répondre aux exigences relatives à la tenue de registres et à la production de rapports.

Échange et enregistrement de renseignements

- Faire en sorte qu'Interpol communique davantage de renseignements sur les crimes économiques internationaux. Interpol devrait envisager d'établir une sous-unité des crimes économiques.

- Évaluer les mécanismes actuels d'entraide juridique afin de déterminer si des efforts additionnels devraient être faits pour lutter contre les crimes économiques.

- Encourager l'établissement de groupes de travail inter-organismes internationaux qui pourront mener des enquêtes sur les crimes économiques.

- Exiger que les institutions financières gardent des registres des opérations effectuées au pays et à l'étranger depuis au moins cinq ans.

Lois sur le secret bancaire

- Examiner les lois sur le secret bancaire afin d'évaluer la nécessité d'établir de nouvelles dispositions, de nouveaux règlements ou autres mesures visant à faciliter l'échange, entre les organismes d'application de la loi, les organismes de réglementation et les divers gouvernements, des registres et autres documents connexes produits par les institutions financières.

Il est trop tôt pour dire si les blanchisseurs d'argent en viendront à s'intéresser à la monnaie électronique. Jusqu'ici, les pays du G-10 n'ont *pas* senti le besoin d'établir de nouvelles dispositions, de nouvelles politiques en matière d'application de la loi ou des mécanismes de coordination officiels portant spécifiquement sur la monnaie électronique. En fait, ils ont plutôt cherché jusqu'ici à surveiller la situation et à rester en contact avec les concepteurs des systèmes de monnaie électronique.

5.0 CONCLUSION

Le succès du Canada au XXI[e] siècle dépendra de notre capacité de participer à l'économie mondiale fondée sur la connaissance. Le gouvernement du Canada entreprend, en partenariat avec le secteur privé et les autres paliers de gouvernement, de nombreuses initiatives à cette fin. Ce partenariat aidera le Canada à tirer profit de la croissance économique qui pourra être réalisée grâce à une approche intelligente en matière de commerce électronique.

Les criminels qui opèrent à l'échelle transnationale pourraient bénéficier considérablement des technologies de la monnaie électronique.

Cependant, ce marché devra être régi par un ensemble de règles clairement définies de manière que les sociétés, les institutions et les individus puissent avoir confiance au système de commerce électronique. Il sera donc fondamental d'assurer la sécurité et la fiabilité de ce système.

Le blanchiment de l'argent par les méthodes traditionnelles constitue déjà un problème grave. Avec les nouvelles technologies de la monnaie électronique, le blanchiment de l'argent risque de prendre une grande ampleur et il deviendra plus compliqué de lutter contre ce fléau.

Les exigences selon lesquelles les paiements électroniques doivent passer par une institution financière (les autorités voulant s'assurer que les opérations ne dépassent pas une certaine limite et qu'il est possible d'identifier les clients) pourraient perdre de leurs effets en raison de la demande accrue pour un service anonyme et des systèmes qui accepteraient des sommes élevées. Ce changement a déjà commencé à s'opérer. Les entreprises qui développent des systèmes de monnaie électronique mettent à l'essai leurs systèmes dans un cadre où il y a moins de restrictions et où les montants limites des opérations sont plus élevés. En fait, dans le cas de certains systèmes, il n'y a aucune limite. Et ce qui est encore plus inquiétant, c'est que certains systèmes permettront d'avoir accès à des sommes et de les transférer sans l'intervention d'une institution financière réglementée.

Avec la monnaie électronique, il serait possible d'effectuer des opérations en espèces dans l'anonymat tout en profitant de la fluidité des communications numériques. Les criminels qui opèrent à l'échelle transnationale pourraient bénéficier considérablement de ces progrès technologiques.

Il ne fait aucun doute que la monnaie électronique jouera aussi un rôle dans d'autres infractions criminelles et sur le plan de la sécurité nationale, par exemple dans les domaines de l'évasion fiscale, de la fraude et de la contrefaçon. De plus, cette technologie soulève des questions qui ne sont pas directement reliées à la justice pénale, comme le risque d'érosion de l'assiette fiscale, la perte de seigneuriage et des préoccupations relatives à la protection de la vie privée.

Les gouvernements pourraient devoir analyser les différents problèmes pouvant découler du blanchiment de l'argent électronique et modifier les lois et règlements actuels et les mécanismes d'application de la loi appliqués actuellement. Il pourrait aussi devenir nécessaire d'accroître la coopération internationale en raison de l'importance et de l'ampleur grandissantes de l'utilisation de la monnaie électronique.

BIBLIOGRAPHIE

Nota : Différents groupes de travail composés de représentants de banques centrales, de ministères responsables des finances et du revenu et d'organismes de réglementation et d'application de la loi ont commencé à définir l'ampleur du problème (voir la bibliographie). Par exemple, Revenu Canada a mis sur pied un comité consultatif sur le commerce électronique composé de représentants de fournisseurs d'accès à Internet, et d'institutions financières, de fiscalistes, d'informaticiens ainsi que de représentants des provinces et des ministères fédéraux visés. Ce comité prévoit déposer son rapport préliminaire au début du printemps.

Mode de présentation des références

Auteurs (collaborateur, société ou entité affiliée). *Titre du document,* titre de la revue ou de l'organisme et adresse Internet s'il y a lieu, numéro de la version ou du dossier s'il y a lieu, date de la dernière mise à jour s'il y a lieu, adresse URL (date d'accès).

ANDERSON, Christopher. A Survey of Electronic Commerce : In Search of the Perfect Market, *The Economist*. http://www.economist.com/surveys/elcom/ec1.html (14 mai 1997)

ANGUS, Ian. Social Engineering for Phone Theft, *Technological Crime Bulletin*, vol. 2, n° 2, sept. 1996, p. 4-6.

BASS, Thomas A. The Future of Money, *Wired Magazine*, vol. 4, n° 10, oct. 1996. http://www.wired.com/wired/4.10/features/wriston.html (28 mai 1997)

BENYEKHLEF, Karim. *Les normes internationales de protection des données personnelles et l'autoroute de l'information,* Justice Canada, juin 1995. http://canada.justice.gc.ca/Conferences/Justice_AE/karim_fr.html (7 mai 1997)

BIRCH, Dave et McEVOY, Neil. DIY Cash, *Wired Magazine*, vol. 2 (avril 1996).

BIRCH, David G.W. Column Five : Bye, Bye Banknotes. *Array Development.* http://www.arraydev.com/commerce/JIBC/9701-12.htm (28 mai 1997)

BORTNER, R. Mark. Cyberlaundering : Anonymous Digital Cash and Money Laundering, University of Miami Law School, 1996. http://www.ovnet.com/~dckinder/documents/cyberlaunder.htm (17 juin 1997)

BOYLES, David. Testimony of David Boyles, Senior Vice President, New Business Ventures, Stored Value Group, and Smart Card Center of Excellence, American Express Travel Related Services, Inc. Before the Subcommittee on Domestic and International Monetary Policy du Committee on Banking and Financial Services, U.S. House of Representatives, 11 juin 1996. http://www.house.gov/castle/banking/dboyles.htm (28 mai 1997)

CANADA. Justice Canada. *Developing a Legal Framework for an Information Age: Cybercrime and Electronic Democracy*, Section de la planification stratégique et des projets spéciaux, Justice Canada, Ottawa.

CANADA. Justice Canada et la Gendarmerie royale du Canada. *Investigation of Computer-Related Crime and Crimes Involving Information Technology*. Meeting of P-8 Senior Experts Group on Transnational Organized Crime, 27-29 novembre 1995, Ottawa, 1995.

CANADA. Larson, Carole. Direction de la sécurité nationale, gouvernement du Canada, document intitulé *Internet Overview*, 12 juin 1997.

CHANNEL ZERO. *The Mondex Scenario : Transcript*, mars 1997. http://www.channel-zero.com/screenings/ch0_cbc/show1/show1.htm (28 mai 1997)

CHAUM, David. *David Chaum's Testimony for US House of Representatives*, DigiCash, 25 juillet 1995. http://www.digicash.com/publish/testimony.html (15 mai 1997)

CHAUM, David. *Prepaid Smart Card Techniques : A Brief Introduction and Comparison*, 1994. http://www.digicash.com/publish/cardcom.html (15 mai 1997)

CHERNEFF, Ruth *et coll. Smart Cards 97*, Shorenet, 1er nov. 1996. http://www1.shore.net/~bauster/cap/s-card/index.html. (28 mai 1997)

Citicorp Suffers First Cyberheist as Regulators Show Alarm, *Money Laundering Alert*, vol. 7, n° 1, oct. 1995, p. 9.

Cleaning Up Dirty Money, *The Economist*, 26 juillet 1997, p. 13-14.

CLINTON, président William T. et vice-président Albert Gore Jr. *A Framework for Global Electronic Commerce*, The President's Information Infrastructure Task Force, 1er juillet 1997. http://www.iitf.nist.gov/eleccomm/ecomm.htm (4 septembre 1997)

COALE, Kristi. EU Selling Swiss Army Smartcard Solution, *Wired News*, 1er février 1997. http://www.wired.com/news/news/technology/story/1814.html (28 mai 1997)

COMMITTEE ON PAYMENT AND SETTLEMENT SYSTEMS. *Security of Electronic Money*, Bank for International Settlement. http://www.bis.org/publ/cpss18.htm (21 mai 1997)

COMMITTEE ON PAYMENT AND SETTLEMENT SYSTEMS. *Security of Electronic Money* (Executive Summary), Bank for International Settlement. http://www.bis.org/publ/cpss18e.htm (12 juin 1997)

COMMITTEE ON PAYMENT AND SETTLEMENT SYSTEMS et GROUP OF COMPUTER EXPERTS OF THE CENTRAL BANKS OF THE GROUP OF TEN COUNTRIES. *Security of Electronic Money*, 1996.

COMMUNITY RESEARCH AND DEVELOPMENT INFORMATION SERVICE (CORDIS). *Conditional Access for Europe : Esprit Project EP 7023*, CORDIS, 20 mars 1997.

Computer crime continues to increase, Reported losses of over $100 million, The Computer Security Institute, 6 mars 1997. http://www.gocsi.com/preleas2.htm (28 avril 1997)

CRYPTOLOGIC INC. *Ecash Operations*, http://www.cryptologic.com/index.html (9 juillet 1997). http://www.cordis.lu/esprit/src/w4w19.htm (6 mai 1997)

DENNING, Dorothy E. *Encryption Policy and Market Trends*, Georgetown University, Department of Computer Science, 11 avril 1997. http://guru.cosc.georgetown.edu/~denning/crypto/Trends.html (2 mai 1997)

DONPA LTD. *AVANT Electronic Purse in Finland*. http://www.sci.fi/%7Edonpa/ep_finla.htm (28 mai 1997)

DORGAN, Michael. Netting Criminals : Financial Officials Try to Stop Illegal Activity from Taking Hold, *San Jose Mercury News*, 24 avril 1996. http://www.sjmercury.com/news/world/cyber423.htm (10 juin 1997)

DUGAS, Sébastyen. Un porte-feuille électronique Mondex, la monnaie du futur, *Direction informatique : Le journal des technologies de l'information*,1996. http://www.direction-informatique.qc.ca/archives/96/04/mondex.html (28 mai 1997)

Electronic Commerce News, vol. 2, n° 25, 23 juin 1997.

ÉTATS-UNIS. Democratic Staff of the Committee on Banking and Financial Services. *Connecting Consumers : Consumer Issues and Emerging Financial Technology*, House Committee on Banking and Financial Services, U.S. House of Representatives, 21 octobre 1996. http://www.house.gov/banking_democrats/consumers.html (31 juillet 1997)

ÉTATS-UNIS. Département des finances. *An Introduction to Electronic Money Issues. Toward Electronic Money and Banking : The Role of Government*, préparé pour la conférence du Département américain des finances, 19-20 septembre 1996, Washington D.C., 1996.

ÉTATS-UNIS. Département des finances. *Exploring the World of Cyberpayments : An Introductory Survey*, 1995.

ÉTATS-UNIS. Département des finances. *Money in Cyberspace: Frequenty Asked Questions*, 3 février 1997. http://www.treas.gov/treasury/bureaus/fincen/cybpage.html (18 juin 1997)

ÉTATS-UNIS. Office of the Comptroller of the Currency, Département des finances. *Toward Electronic Money & Banking : The Role of Government,* une conférence parrainée par le Département des finances, Washington D.C., 19-20 septembre 1996. http://www.occ.treas.gov/emoney.htm (11 mars 1997)

ÉTATS-UNIS. Subcommittee on Domestic and International Monetary Policy, U.S. House of Representatives. *Submission to the US House of Representatives by Mondex on 'The Future of Money',* 11 juin 1996, U.S. House of Representatives. http://www.house.gov/castle/banking/jones.htm (28 mai 1997)

ÉTATS-UNIS. Subcommittee on Domestic and International Monetary Policy, U.S. House of Representatives. Testimony of Professor James L. Brown, Director, Center for Consumer Affairs, University of Wisconsin, Milwaukee, before the Subcommittee on Domestic and International Monetary Policy of the Committee on Banking and Financial Services, US House of Representatives. Regarding Implications of Electronic Banking and Commerce, U.S. House of Representatives, 7 mars 1997. http://www.house.gov/castle/banking/brown3.htm (31 juillet 1997).

EUROPAY INTERNATIONAL. *Europay Launches the World's First Multi-Currency Electronic Purse 'Clip' : Paves Way for Making Secure, Convenient, Low-value Purchases Internationally,* 20 juin 1996. http://www.europay.com/1996/ph6rtt0y.htm (28 mai 1997)

EUROPAY INTERNATIONAL. *The Use of Chip to Meet Consumer Demand : Europay International Members Meeting, Séville, 1996,* 20 juin, 1996. http://www.europay.com/1996/ph6rtt1b.htm (28 mai 1997)

EUROPAY (Suisse). *CASH Resolves Problems with Small Change,* 29 janvier 1997. http://www.eurocard.ch/english/news/press1.html (28 mai 1997)

EUROPEAN COMMITTEE ON CRIME PROBLEMS (CDPC). Committee of Experts on Crime in Cyberspace (PC-CY). *Problems of Legislation in the Area of Computer-related Crime,* présenté par M. M. Möhrenschlager (ministre de la Justice, Allemagne) au International Symposium on Comparative Law, Recent Developments in Public Affairs, Istanbul, 1996

FEDERAL RESERVE BANK OF DALLAS. *How Do We Pay?,* premier trimestre de 1997. http://www.dallasfed.org/publications/fi/txt/fi_97_1q.html (28 mai 1997)

FIRST VIRTUAL. *Buying Summary,* http://www.fv.com/info/buyerintro.html. (2 juillet 1997)

FRIED, FRANK, HARRIS, SHRIVER ET JACOBSON. Statement of Thomas P. Vartanian, Partner of Fried, Frank, Harris, Shriver & Jacobson, Before the Federal Deposit Insurance

Corporation, Concerning Stored Value Cards and Electronic Payment Systems, 12 Septembre 1996. http://ffhsj.com/bancmail/tpvtest.htm (28 mai 1997)

FROOMKIN, A. Michael. *Flood Control on the Information Ocean : Living With Anonymity, Digital Cash, and Distributed Databases,* University of Miami Law School. http://www.law.miami.edu/~froomkin/articles/oceanno.htm (31 juillet 1997)

FROOMKIN, Michael. *The Unintended Consequences of E-Cash,* University of Miami Law School, version 1.2, 12 mars 1997. http://www.law.miami.edu/~froomkin/articles/cfp97.htm (31 juillet 1997)

FROST, Mark. *A Brief Introduction to the Digitalization and Globalization of Money and Capital,* Toronto,18-22 mars 1997.

G7 Groups Frets Over Electronic Money Laudering, *The Nando Times*, 6 février 1997. http://www.nando.net/newsroom/ntn/info/020697/info8_2320.html (26 mai 1997)

GOLDFINGER, Charles (Financial Issues Working Group (FIWG*). Electronic Money in the United States : Current Status, Prospects and Major Issues,* Fact-finding Mission for the Financial Issues Working Group of the European Commission, 25 août-5 sept. 1996, Information Society Project Office (ISPO), 8 janvier 1997. http://www.ispo.cec.be/infosoc/eleccom/elecmoney.html (6 mai 1997)

GRIGG, Ian. *Critique on the 1994 EU Report on Prepaid Cards,* Systemics Software Archive Document Library, nov.- déc. 1996. http://www.systemics.com/docs/papers/1994_critique.html (28 mai 1997)

GROUPE DES DIX. *Electronic Money : Consumer Protection, Law Enforcement, Supervisory and Cross Border Issues*, rapport du Groupe de travail sur la monnaie électronique, 1997. (Peut être consulté sur le site Web : http://www.bis.org)

HALLAM-BAKER, D[r] Phillip M. *Electronic Payment Schedules,* World Wide Web Consortium (W3C). http://www.w3.org/Payments/roadmap.html (20 août 1997)

HANNAFORD, sergent Craig. Electronic Cash, *Technological Crime Bulletin*, vol. 2, n° 2, septembre 1996, p. 5.

HARRIS, Holly. *La vie privée et l'autoroute de l'information,* juin 1995, Justice Canada. http://canada.justice.gc.ca/Conferences/Justice_AE/harris_fr.html (7 mai 1997)

HOENIG, Thomas M. The Evolution of the Payments System : A U.S. Perspective, *Economic Review,* Federal Reserve Bank of Kansas City (troisième trimestre de1995), p. 5-9.

HUGHES, Sarah Jane. Cyberlaundering Poses Threat to Controls, *Money Laundering Alert*, vol. 6, n° 7, avril 1995, p. 1-6.

HUGHES, Sarah Jane. Phantom Cyberbanks Pose Laudering, Tax Evasion Threat, *Money Laundering Alert*, vol. 6, n° 10, juillet 1995, p. 4.

INFO-SEC.COM. *German Law on Encrypted Telecommunications Examined*, 28 mars 1997. http://www.info-sec.com/crypto/crypto_i.html-ssi (2 mai 1997)

INTERCASINO. InterCasino, http://www.intercasino.com/about/index.html (9 juillet 1997)

INTERNATIONAL EXPERT GROUP ON MISUSE OF INTERNATIONAL DATE NETWORKS. *Declaration of the Expert Group on Misuse of International Data Networks of the G7 Ministers of Science (Carnegie Group)*, première rencontre, Bonn 27-29 nov. 1996, version 1.0, 1997.

Internet could become dirty money haven, *The Nando Times*, 14 mars 1996. http://www.nando.net/newsroom/ntn/info/031496/info3_11722.html (26 mai 1997)

JAMIESON, Caporal Gordon. Wireless Fraud : The Global Perspective, *Technological Crime Bulletin*, vol. 2, n° 2, sept. 1996, p. 1-6.

JOHNSON, James A. *Report on Organization*, United States National Information Infrastructure Virtual Library, mars 1997. http://nii.nist.gov/pubs/intl_org.html (6 mai 1997)

McKAY, Sam et KALIN, Sari. Will You Soon be Using Smart Cards for Electronic Payments?, *SunWorld*, vol. 11, n° 3, 12 mars 1997. http://www.eimb.rssi.ru/sunworldonline/swol-03-1997/swol-03-att.html (22 mai 1997)

McNEIL, Mark. Privacy up for Sale in a Buyer's Market : Electronic Trail Left Behind as Credit Purchases Sell Out User, *The Hamilton Spectator*, vol. 3, avril 1997. http://insight.dcss.mcmaster.ca/org/efc/pages/media/spectator.03apr97.html (22 mai 1997)

MEISTER, Edgar. (traduction et commentaires de Kuner, Christopher Esq.), Speech by Bundesbank Director Edgar Meister on Electronic Cash, 28 nov. 1996, *Ourworld*. http://ourworld.compuserve.com/homepages/ckuner/meister.htm#meister (28 mai 1997)

MONDEX INTERNATIONAL. Credit Union Central of Canada Joining Banks in Offering Mondex Electronic Cash, *Mondex International Press Releases*, 6 février 1997. http://www.mondex.com/mondex/cgi-bin/show.pl?english+global&../english/documents/global/prel45243922.txt (28 mai 1997)

MONDEX INTERNATIONAL. MasterCard International Completes 50 Per Cent Acquisition of Mondex International, *Mondex International Press Release*, 23 février 1997. http://www.mondex.com/mondex/cgi-

bin/show.pl?english+global&../english/documents/global/prel61885785.txt (28 mai 1997).

Money Laundering : That Infernal Washing Machine, *The Economist,* 26 juillet 1997, p. 19-21.

MORRIS, Stanly E. Observations de Stanley E. Morris, directeur, Financial Crimes Enforcement Network, Département américain des finances, devant le forum sur les services financiers, Groupe d'action financière international, Paris, France, 1996.

MULLER John D. *Selected U.S. Legal Issues in Issuance of Electronic Money.* http://www.brobeck.com/docs/0497first.html (31 juillet 1997)

OURWORLD. *Report to the Council of the European Monetary Institute on Prepaid Cards by the Working Group on EU Payment Systems,* mai 1994. http://ourworld.compuserve.com/homepages/ckuner/prepaid.htm (28 mai 1997)

PIRAGROFF, Donald et HOLHUIS, Annemieke. *Les nids-de-poule de l'autoroute électronique : Crimes et abus,* Justice Canada, juin 1995. http://canada.justice.gc.ca/Conferences/Justice_AE/piragoff_fr.html (7 mai 1997)

PORTEOUS, Sam. *Le crime organisé étude d'impact – Points saillants.* Ministre des Travaux publics et services gouvernementaux Canada, 1998.

PORTEOUS, Sam. *Transnational Organized Crime and E-cash*, mémoire non classifié SCRS.

POST, David G. *Anarchy, State, and the Internet : An Essay on Law-Making in Cyberspace* (article 3), Cornell Law School, Legal Information Institute, 1995. http://www.law.cornell.edu/jol/post.html (1er mai 1997)

POST, professeur David G. *Law of Cyberspace Seminar,* Cyberspace Law Institute, automne 1996. http://www.cli.org/cyberspace/index.html (1er mai 1997)

PRIVACY INTERNATIONAL. *Privacy Internationals Mondex Complaint is Upheld: Electronic Cash is Anything but Anonymous,* Privacy International, 21 juin 1997. http://www.privacy.org/pi/activities/mondex/mondex_release.html (28 mai 1997)

QUEAU, Philippe. Qui contrôlera la cyber-économie?, *Le Monde diplomatique*, février 1995. http://www.monde-diplomatique.fr/md/1995/QUEAU/1160.html (27 mars 1997)

QUIRK, Peter J. Money Laundering : Muddying the Macroeconomy, *Finance & Development*, mars 1997. http://www.worldbank.org/fandd/english/abstract/0397/011a0397.htm (31 juillet 1997)

Recommendation No R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with Information Technology,

Electronic Frontier Foundation, 29 septembre 1995. http://www.eff.org/pub/Global/Multinational/Privacy/ce_privacy_search_r95-13.recommendations (6 mai 1997)

REUTERS LTD. BankAmerica, VISA to Start Internet Test, *Yahoo! News*, 16 mai 1997. http://www.yahoo.com/headlines/tech/stories/bankamerica_1.html (16 mai 1997)

RICHARDS, Scott. *Electronic Money/Internet Payment Systems,* Electronic Banking Resource Center. http://www2.cob.ohio-state.edu/~richards/bankpay.htm, 25 juin 1997.

SERVIDA, Andrea. *Electronic Commerce - Security Related Projects (mostly in 4th FP).* CORDIS, 19 mars 1997. http://www.cordis.lu/esprit/src/w4w15.htm (6 mai 1997)

Shining a Light on Privacy, *Government Computer*, avril 1997, p. 8, 10-11.

SIEBER, Dr Ulrich. *Research Proposal on Legal Aspects of Computer-Related Crime in the Information Society,* Würzburg.

SIEBER, Dr Ulrich. EC-Research Project, *Computer-related Crime* (COMCRIME), n° 1 General Information and Questionnaire for the Country Reports, Würzburg.

TASK FORCE ON STORED-VALUE CARDS. A Commercial Lawyer's Take on the Electronic Purse : An Analysis of Commercial Law Issues Associated with Stored-Value Cards and Electronic Money, *The Business Lawyer*, vol. 52, n° 2, février 1997, p. 653-727.

TAYLOR, Ian. *Licensing of Trusted Third Parties for the Provision of Encryption Services : Public Consultation Paper on Detailed Proposals for Legislation,* Department of Trade and Industry, Internet Services (UK), mars 1997. http://dtiinfo1.dti.gov.uk/pubs (2 mai 1997)

TD BANK. Visa, Scotiabank and TD Bank Announce Canadian Trial of Reloadable Visa Cash Card, *TD Bank Press Releases*, 15 avril 1997. http://www.tdbank.ca/tdbank/Press_Rel/apr15a97.htm (28 mai 1997)

The Economist. The Disappearing Taxpayer, *The Economist,* 1997. http://www.economist.com/issue/1-05-97/ld4660row.html (4 juin 1997)

The Economist. Disappearing Taxes : The Tap Runs Dry, *The Economist,* 31 mai 1997. http://www.economist.com/issue/31-05-97/sf0879.html (4 juin 1997)

The Economist. Chipper, For Now, *The Economist,* 26 avril 1997. http://www.economist.com/issue/26-04-97/fn6691.html (28 mai 1997)

The Economist. Going for Olympic Gold Cards, *The Economist,* 30 mars 1997. http://www.economist.com/issue/30-03-96/fnl.html (28 mai 1997)

The First Bank of Internet. *The First Bank of Internet,* 20 mars 1995. http://www.cs.nps.navy.mil/curricula/tracks/security/homework/FBOI.txt (2 juillet 1997)

TREND MONITOR. *Beyond Money : The Implications of Electronic Cash and Virtual Banking.* http://www.trendmon.demon.co.uk/eesa.htm (28 juillet 1997)

VAN DER WIELEN, Henry. *Electronic Money : A European Perspective,* Systemics Software Archive Document Library, 4 février 1997. http://www.systemics.com/docs/papers/EU_perspective.html (31 juillet 1997)

VAN HOVE, Leo. *A Selected Bibliography on Electronic Purses,* Leo Van Hove - bibliography on electronic purses. http://cfec.vub.ac.be/cfec/purses.htm (28 mai 1997)

WAHLERT, Glenn. Money Laundering, the Perils of Cyberpayments, *Technological Crime Bulletin*, vol. 2, n° 2, septembre 1996, p. 2-3.

*** ***D'autres sources ont parfois été consultées.***

ANNEXE I
LE FONCTIONNEMENT DES SYSTÈMES DE MONNAIE ÉLECTRONIQUE
(Les renseignements donnés valent pour la plupart des systèmes actuels.)

On entend par « monnaie électronique » une monnaie portant la signature numérique de l'établissement émetteur qui a utilisé à cette fin une clé de cryptage confidentielle. Cette monnaie est transmise au client, qui peut s'en servir pour payer électroniquement des biens et des services partout dans le monde.

- Au moyen d'Internet et à partir de son ordinateur personnel, l'utilisateur demande de la monnaie électronique en entrant en communication avec sa banque et en certifiant qu'il est le titulaire du compte.

- Une fois qu'il a certifié qu'il est le titulaire du compte, l'utilisateur présente une demande à l'aide d'une clé de cryptage aléatoire dans une enveloppe numérique protégée.

- La banque appose sa signature numérique (authentifiant ainsi la monnaie électronique pour le bénéficiaire éventuel) et l'utilisateur en reçoit la confirmation.

- L'utilisateur peut alors télécharger la monnaie dans sa carte intelligente à l'aide d'un périphérique semblable à un guichet automatique, ou bien il peut transférer ou dépenser cette monnaie sur Internet comme il le ferait pour un message transmis par courrier électronique.

- Les bénéficiaires n'ont qu'à mémoriser la monnaie électronique et à ajouter, au moyen de leur ordinateur, le code d'identification de leur compte. Ils peuvent télécharger la monnaie dans une carte intelligente ou la transférer dans leur compte bancaire.

Autre système de monnaie électronique

La monnaie électronique peut faire l'objet d'un échange en ligne entre deux parties, sans l'intervention d'un tiers. Les porte-monnaie électroniques découlent d'une technologie différente; il ne s'agit en fait que d'une monnaie prépayée.

Le porte-monnaie électronique peut être décrit comme suit :
Il s'agit d'une carte intelligente prépayée dans laquelle une valeur a été mémorisée et dont le titulaire peut se servir pour régler ses achats chez des détaillants. Les détaillants qui acceptent ces cartes sont remboursés périodiquement avec de la monnaie traditionnelle par les fournisseurs du système. Ces fournisseurs reçoivent à l'avance de l'argent des titulaires de ces cartes et mémorisent la valeur correspondante dans les cartes. Dans chacun de ces trois types d'opérations, des données protégées représentant une valeur sont échangées contre de l'argent ou contre des biens ou services. (Chaum, 1994)

Les cartes d'appel, les cartes qui remplacent la petite monnaie dans les universités et les systèmes de paiement dans les stations de ski sont des exemples de porte-monnaie électroniques simples. Durant les Jeux olympiques d'Atlanta, des cartes semblables mais plus perfectionnées ont été distribuées à plus de 300 000 personnes.

Il y a quatre principaux types de technologie :

Les cartes à mémoire - Ces cartes servent uniquement à mémoriser des données (elles n'ont pas de fonction de calcul). Elles renferment un programme pour les besoins du NIP.

Les cartes à clés partagées - Grâce à des clés intégrées à une puce, la carte peut communiquer avec tout autre dispositif qui possède les mêmes clés. (Chaum, 1994)

Les cartes porte-signature - Ces cartes sont semblables aux cartes à clés partagées, mais elles renferment un programme légèrement différent. Une signature numérique y est mémorisée. Chaque fois que la carte est utilisée, le fournisseur du système introduit la signature numérique comme s'il libellait un chèque.

Les cartes-signatures - Ces cartes sont presque identiques aux cartes porte-signature. Cependant, la puce qui s'y trouve renferme une signature numérique. Le fournisseur du système n'a donc pas à l'introduire.

ANNEXE II
CRYPTOGRAPHIE ET COMMERCE ÉLECTRONIQUE

La cryptographie (ou encryptage) est particulièrement importante pour la croissance du commerce électronique car elle permet d'assurer l'authenticité, l'intégrité et la confidentialité des opérations et des communications, rendant ainsi sécuritaires les communications numériques.

La cryptographie consiste à remplacer des chiffres et des lettres par d'autres chiffres et lettres afin de rendre le message ou la communication incompréhensible. Il faut des clés pour le cryptage et le décryptage de ces messages ou communications.

Les criminels et les terroristes peuvent assez facilement utiliser la cryptographie pour faire obstacle au travail de collecte de renseignements des organismes d'application de la loi et des agences de sécurité. Par exemple, des éléments de preuve qui ont été chiffrés sont incompréhensibles s'ils ne sont pas déchiffrés. L'incapacité de décoder ces éléments pourrait avoir de graves conséquences sur la prévention, le dépistage, les enquêtes et les poursuites ainsi que sur la capacité du gouvernement canadien d'exercer une surveillance à l'égard des menaces à la sécurité des Canadiens. C'est pour ces raisons que l'on préconise que des limites raisonnables soient fixées pour la production, l'exportation, l'importation et l'utilisation des techniques de cryptographie.

(Pour une analyse plus détaillée de la question de la cryptographie, voir le document de travail intitulé *Politique cadre en matière de cryptographie aux fins du commerce électronique : Pour une économie et une société de l'information au Canada,* Industrie Canada, février 1998.)

ANNEXE III
CARACTÉRISTIQUES DES SYSTÈMES DE PAIEMENT QUELQUES GÉNÉRALISATIONS SUCCINCTES AUX FINS DE LA DISCUSSION

Systèmes de paiement actuels	Systèmes de cyberpaiement
• Degré élevé de contrôle des banques centrales	• Approches nationales différentes à l'égard du contrôle
• Surveillance et réglementation très structurées	• À déterminer - aspects très techniques
• Abondante documentation sur les questions juridiques et les politiques	• Degré moindre de règlements
• Vérification et mécanismes mis en place aux douanes	• Pas encore de technologie pour la surveillance
• Modes de paiement traditionnels - chèques, monnaie	• Paiements électroniques intangibles
• Infrastructure imposante partout dans le monde	• Réduction des effectifs due à l'informatisation
• Densité de main-d'oeuvre relativement forte	• Intensité relative du capital
• Infrastructure de grande valeur - solide	• Installations décentralisées à faible coût
• Virements télégraphiques effectués surtout par les banques	• Virements au moyen d'un ordinateur personnel
• Paiements effectués surtout par chèque	• Prédominance de la cybermonnaie
• Faible vélocité de la monnaie	• Forte vélocité de la monnaie
• Intermédiaires - surtout les banques	• Disparition des intermédiaires traditionnels
• Mécanismes de compensation nécessaires	• Moins grand besoin de mécanismes de compensation
• Transport par messager, transport routier, maritime ou aérien	• Télécommunications
• Utilisation de la devise américaine partout dans le monde	• Change facile - une seule monnaie

• Numéros de série et relevés bancaires	• Messages chiffrés
• Collecte importante de données statistiques	• Aucune méthode pour la collecte de statistiques sur Ms
• Frontières économiques nationales	• Aucune frontière
• Juridiction bien définie	• Chevauchement, juridiction non définie
• Méthodes de validation uniformisées, généralement reconnues	• Évolution constante des méthodes de vérification des opérations
• Caractère fongible	• Convertibilité propre au système pour l'obtention d'argent
• Structure établie pour l'authentification	• Non déterminé - intervention d'un tiers nécessaire dans certains systèmes

ANNEXE IV
APERÇU DES POLITIQUES SUR LA MONNAIE ÉLECTRONIQUE ÉTABLIES PAR LES PAYS DU G-10

Inventaire des politiques à l'égard de la monnaie électronique dans les pays du G-10

Pays	Fraude, perte, vol, litiges	Obligations d'information
Allemagne	Application générale du code civil. Programme d'ombudsman.	Application générale du code civil et des règles régissant les établissements de crédit.
Belgique	Application générale du Code civil et des règles régissant les établissements de crédit. Le programme volontaire de l'ombudsman pour le règlement des litiges, mis sur pied par l'association des banques, peut s'appliquer à la monnaie électronique.	Application générale du Code civil et des règles régissant les établissements de crédit.
Canada	Application générale du Code civil et des règles régissant les établissements de crédit. Ombudsman de la profession bancaire. L'association professionnelle élabore des normes sur la sécurité contre la fraude et le vol pour la monnaie électronique, notamment les porte-monnaie électroniques.	Information obligatoire sur tous les frais de service reliés aux comptes de banque, de fiducie et de sociétés de prêts, y compris sur les frais pour les transferts électroniques de fonds en provenance de comptes de dépôt. Il faut également donner de l'information sur les droits et obligations des consommateurs en ce qui concerne les cartes de crédit.
États-Unis	Application générale du droit commercial. Application de l'Electronic Fund Transfer Act (Loi sur les transferts électroniques de fonds) aux porte-monnaie électroniques en cours d'examen par la Federal Reserve.	Application des obligations d'information de l'Electronic Fund Transfer Act aux porte-monnaie électroniques en cours d'examen par la Federal Reserve. L'Office of the Comptroller of the Currency a établi des directives pour les banques nationales.
France	Application générale du Code civil (erreurs et litiges) et des règles régissant les établissements de crédit (s'appliquant actuellement à la perte et au vol de chèques et de cartes de crédit).	Application générale du Code civil et des règles régissant les établissements de crédit.
Italie	Application générale du code civil et de la loi de 1993 sur les banques. Code d'autoréglementation de la profession bancaire, applicable aux systèmes de monnaie électronique. Ombudsman de la profession bancaire pour le règlement des litiges.	Les autorités de contrôle projettent d'exiger qu'une information détaillée soit donnée aux consommateurs.
Japon	Application générale du code civil et des règles régissant les établissements de crédit. Les entités financières et les sociétés de technologie ont élaboré des normes techniques pour prévenir la fraude, la	Application générale du code civil et des règles régissant les établissements de crédit. La loi sur les cartes prépayées prévoit que

	perte et le vol pour les systèmes informatiques des établissements financiers.	les limites sur la durée ou le territoire d'utilisation doivent être indiquées sur la carte.
Pays-Bas	Les procédures de solution des litiges des tribunaux et du comité de la profession bancaire s'appliquent à la monnaie électronique. Code des meilleures pratiques de la profession bancaire sur la protection du consommateur. Le gouvernement hollandais reconnaît les mesures d'autoréglementation.	Application générale du code civil et des règles régissant les établissements de crédit.
Royaume-Uni	Règlement des litiges et clauses abusives traités dans le Fair Trading Act (Loi sur les pratiques commerciales loyales) et l'Unfair Terms in Consumer Contracts Act (Loi sur les clauses abusives dans les contrats de consommation). Le Code of Banking Practice (Code des pratiques bancaires) couvre la perte et les erreurs dans les cas où des banques ou des mutuelles d'épargne et de construction sont impliquées. Programme d'ombudsman volontaire pour les banques et obligatoire pour les mutuelles d'épargne et de construction.	Les dispositions générales du Code of Banking Practice (Code des pratiques bancaires) s'appliquent aux banques et aux mutuelles d'épargne et de construction.
Suède	Application générale du code civil et des règles régissant les établissements de crédit.	Application générale du code civil et des règles régissant les établissements de crédit.
Suisse	Application générale du Code civil et du Code pénal.	Application générale du Code civil.

Pays	**Règles prudentielles applicables aux émetteurs**	**Inspections, contrôles internes et sécurité des systèmes d'information**
Allemagne	Règles ordinaires de fonds propres, de solvabilité et de liquidité pour les établissements de crédit qui acceptent des dépôts et consentent des prêts. Règles modifiées possibles pour les établissements qui ne font qu'émettre de la monnaie électronique.	Les établissements de crédit présentent un rapport mensuel à la Bundesbank, ainsi que des comptes annuels, un rapport annuel et un rapport du vérificateur aux FBA et à la Bundesbank.
Belgique	Mêmes règles pour les établissements de crédit que pour les autres activités bancaires.	Procédures applicables aux établissements de crédit. La Banque nationale de Belgique collecte des informations statistiques auprès des exploitants de systèmes de monnaie électronique deux fois par année. Elle a procédé à une vérification officieuse du système de monnaie électronique.
Canada	Dans le cas des institutions financières réglementées, la législation et la réglementation existantes, notamment en ce qui concerne les fonds propres, s'appliquent.	Procédures applicables aux institutions financières réglementées.

États-Unis	Pas de règles financières particulières pour les banques qui émettent de la monnaie électronique. Certains États prescrivent des normes de placement pour les établissements non bancaires de transfert de fonds; l'application de ces normes aux émetteurs de monnaie électronique est incertaine.	Inspections des banques sur place, généralement une fois par année, portant sur la sécurité des systèmes d'information, les contrôles internes, etc. L'habilitation en matière d'inspection couvre la société de portefeuille qui possède une banque et les filiales de banques. Certains États procèdent à des inspections des établissements non bancaires de transfert de fonds ou leur imposent d'autres règles.
France	Réglementation bancaire ordinaire.	Même procédures pour les établissements de crédit (inspections sur place, contrôles internes, vérification de la sécurité informatique)
Italie	Mêmes règles que pour les autres activités bancaires.	Règles ordinaires en matière d'inspections et de rapports applicables aux établissements de crédit. Les systèmes de monnaie électronique sont soumis à des contrôles non sur place. La Banque d'Italie envisage l'introduction de règles en matière de sécurité des systèmes d'information et de contrôle interne.
Japon	Les établissements de crédit sont soumis aux règles de la loi sur les banques. Les émetteurs soumis à la loi sur les cartes prépayées doivent déposer auprès du bureau des dépôts des fonds correspondant à 50 % au moins des soldes inutilisés des cartes émises.	Les établissements de crédit sont soumis aux règles ordinaires en matière d'inspections et de rapports. Les émetteurs soumis à la loi sur les cartes prépayées sont assujettis aux règles ordinaires en matière de rapports et, pour les émetteurs tiers, d'inspections.
Pays-Bas	Les émetteurs doivent se conformer à toutes les dispositions de la loi sur la surveillance du système de crédit, y compris les règles de liquidité et de fonds propres.	Mêmes procédures pour les établissements de crédit, y compris en matière de qualification, de direction et d'obligations pour l'exploitant du système de respecter les règles de sécurité et d'intégrité du système de monnaie électronique. Inspections sur place et non sur place et vérifications externes
Royaume-Uni	Les lois et la réglementation bancaires ordinaires s'appliquent aux banques.	Les banques et les mutuelles d'épargne et de construction doivent établir qu'elles ont un plan d'activité réaliste ainsi que des systèmes et des contrôles suffisants.
Suède	Les lois et la réglementation bancaires ordinaires s'appliquent aux banques.	Les règles bancaires ordinaires s'appliquent. Inspections sur place et non sur place et vérifications externes
Suisse	La Loi sur les banques définit les règles financières pour les banques, soumises au contrôle de la Commission fédérale des banques.	Rapports du réviseur pour les banques. Le Code des obligations soumet les autres sociétés à une procédure d'inspection de manière à respecter la norme commune pour la profession.

Pays	Autorisation
Allemagne	L'émission de monnaie électronique est réservée aux établissements de crédit, sauf en ce qui concerne les cartes prépayées de clientèle (à deux parties). Les établissements de crédit de plein exercice n'ont pas besoin d'autorisation particulière pour émettre des cartes prépayées ou de la monnaie pour réseau électronique. L'émetteur de carte prépayée universelle peut être dispensé de l'agrément par le bureau de surveillance de la Banque fédérale.
Belgique	À l'heure actuelle, aucune restriction légale sur l'émission de monnaie électronique. Jusqu'à maintenant, seuls les établissements de crédit ont émis de la monnaie électronique. Ces établissements n'ont pas besoin d'autorisation particulière pour émettre de la monnaie électronique.
Canada	À l'heure actuelle, rien n'interdit aux établissements non financiers d'émettre de la monnaie électronique (toutefois, seules des institutions financières de dépôt, réglementées, ont émis de la monnaie électronique jusqu'à maintenant). Il se peut qu'une institution financière doit obtenir une approbation en vue d'établir une filiale.
États-Unis	Les banques n'ont pas besoin d'autorisation particulière pour émettre des produits de monnaie électronique. Cependant, une banque peut avoir besoin d'une autorisation pour investir dans une entité distincte en vue d'exercer ces activités. Les lois des États sur les établissements de transfert de fonds peuvent obliger les établissements autres que les établissements de dépôt à obtenir l'agrément pour émettre de la monnaie électronique.
France	La loi bancaire réserve aux établissements de crédit l'émission de monnaie électronique, sauf en ce qui concerne les cartes prépayées de clientèle. Les établissements de crédit n'ont besoin d'aucune autorisation particulière pour émettre de la monnaie électronique, mais tout système doit être soumis à la Banque de France.
Italie	L'émission de cartes universelles est réservée aux établissements de crédit. Les établissements de crédit n'ont pas besoin d'autorisation particulière.
Japon	À l'heure actuelle, l'émission de monnaie électronique rachetable en espèces est limitée aux établissements de crédit; cette politique est en voie de révision. Selon la loi sur les cartes prépayées, les émetteurs de cartes à deux parties (l'émetteur et le marchand doivent être la même personne) doivent notifier le ministère des Finances; les émetteurs de cartes à trois parties (c.-à-d. autres que les cartes à deux parties) doivent s'inscrire auprès du ministère des Finances.
Pays-Bas	Les émetteurs de monnaie électronique sont considérés comme des établissements de crédit, qui doivent être agréés par la Banque des Pays-Bas. Des exceptions sont possibles dans le cas de petits systèmes de monnaie électronique. Les entités qui interviennent dans la mise en œuvre d'un système de monnaie électronique, sans être elles-mêmes des émetteurs de monnaie électronique, ne sont pas considérées comme des établissements de crédit.
Royaume-Uni	Les banques sont assujetties à une autorisation générale selon le Banking Act (Loi sur les banques) et les mutuelles d'épargne et de construction, selon le Building Societies Act (Loi sur les mutuelles d'épargne et de construction). Les émetteurs de monnaie électronique autres que les banques, s'ils ne présentent pas les caractéristiques liées à la réception de dépôts, n'auraient pas besoin d'autorisation. Quant à ceux qui présentent ces caractéristiques, ou bien ils devront demander eux-mêmes une autorisation, ou bien ils devront former une coentreprise avec un établissement autorisé, lequel sera responsable de la réception de dépôts.

Suède	À l'heure actuelle, aucune restriction sur l'émission de monnaie électronique. Les banques n'ont pas besoin d'autorisation particulière. Jusqu'à maintenant, les banques et les établissements de crédit ont été les seuls à émettre de la monnaie électronique.
Suisse	Les autorités n'ont pas encore pris de position sur l'émission de monnaie électronique. Jusqu'à maintenant, les banques et la Poste suisse participent à des systèmes de monnaie électronique universelle. Selon la position de la Commission fédérale des banques, l'émission de monnaie électronique est liée à l'offre d'accepter des dépôts du public à titre professionnel, activité réservée aux banques. La législation envisagée en matière de blanchiment de capitaux obligera les émetteurs de monnaie électronique à faire partie d'un organisme d'autoréglementation ou à obtenir l'agrément d'un organisme public spécialisé.

Pays	**Mesures contre le blanchiment de capitaux**
Allemagne	Les lois et règlements sur le blanchiment des capitaux s'appliquent aux établissements de crédit.
Belgique	Les lois contre le blanchiment des capitaux s'appliquent aux établissements de crédit.
Canada	Les mesures contre le blanchiment des capitaux s'appliquent si l'émetteur est une institution financière réglementée.
États-Unis	Les lois et règlements sur le blanchiment des capitaux s'appliquent aux établissements de crédit et aux autres établissements. Leur application aux produits de monnaie électronique est en cours de révision.
France	Les lois et règlements sur le blanchiment des capitaux s'appliquent aux établissements de crédit.
Italie	Les lois et règlements sur le blanchiment des capitaux s'appliquent aux établissements de crédit.
Japon	Les lois et règlements sur le blanchiment des capitaux s'appliquent aux établissements de crédit et aux autres établissements.
Pays-Bas	La loi sur le blanchiment des capitaux s'applique, notamment la règle sur la connaissance du client et la déclaration des opérations inhabituelles.
Royaume-Uni	Les Money Laundering Regulations (Règlement sur le blanchiment des capitaux) de 1993 s'appliquent à la monnaie électronique. Obligation de déclarer les opérations suspectes et d'être en mesure de fournir une piste de vérification.
Suède	Les lois et règlements sur le blanchiment des capitaux s'appliquent aux établissements de crédit.
Suisse	La loi envisagée sur le blanchiment des capitaux s'appliquera à tous les intermédiaires financiers, y compris les émetteurs de monnaie électronique. Ce texte obligera les intermédiaires financiers à fournir toute l'information nécessaire pour reconstituer les opérations.

Pays	**Assurance-dépôts ou autres garanties**	**Protection des renseignements personnels**
Allemagne	Règles pour les établissements de crédit.	Application générale du code civil.
Belgique	L'application du régime d'assurance-dépôts aux produits de monnaie électronique est en cours de révision.	Le droit belge incorpore la directive de la CE sur la protection des données à caractère personnel.

Canada	L'application du régime d'assurance-dépôts aux produits de monnaie électronique est en cours de révision.	Règlements à venir en 1997 pour les institutions financières de réglementation fédérale. Une loi générale sur la protection des renseignements personnels sera élaborée par le gouvernement fédéral pour l'an 2000. Le Québec a adopté une loi sur la protection des renseignements personnels dans le secteur privé. Les institutions financières vont adopter en 1997 le Code sur la protection des renseignements personnels de la CSA. L'Association canadienne des paiements impose des obligations générales de protection des renseignements personnels.
États-Unis	Application générale du droit commercial. L'application de l'Electronic Fund Transfer Act (Loi sur les transferts électroniques de fonds) aux porte-monnaie électroniques est en cours d'examen par la Federal Reserve.	Application des obligations d'information de l'Electronic Fund Transfer Act aux porte-monnaie électroniques en cours d'examen par la Federal Reserve. L'Office of the Comptroller of the Currency a établi des directives pour les banques nationales.
France	Le régime d'assurance-dépôts s'applique à la monnaie électronique.	Application générale du Code civil. Application de la loi bancaire française. Le consentement du consommateur est nécessaire pour le transfert de renseignements personnels.
Italie	Le régime d'assurance-dépôts s'applique à la monnaie électronique. Les cartes au porteur sont exclues.	La directive de la CE a été récemment mise en œuvre par le Parlement.
Japon	L'application du régime d'assurance-dépôts à la monnaie électronique est en cours de révision. En vertu de la loi sur les cartes prépayées, les titulaires de carte ont priorité sur les fonds que les émetteurs doivent déposer auprès du bureau des dépôts.	Des groupes professionnels ont établi des directives détaillées sur la protection des renseignements personnels pour les établissements financiers.
Pays-Bas	L'application du régime d'assurance-dépôts à la monnaie électronique est à l'étude. Les banques qui participent à des systèmes de monnaie électronique ont élaboré un plan de partage des pertes en cas d'insolvabilité de l'un des membres du groupe.	La loi hollandaise sur l'enregistrement des données à caractère personnel et la directive de la CE s'appliquent à la monnaie électronique.
Royaume-Uni	Règlement des différends et clauses abusives traités dans le Fair Trading Act (Loi sur les pratiques commerciales loyales) et l'Unfair Terms in Consumer Contracts Act (Loi sur les clauses abusives dans les contrats de consommation). Le Code of Banking Practice (Code des pratiques bancaires) couvre la perte et les erreurs dans les cas où des banques ou des mutuelles d'épargne et de construction sont	Les dispositions générales du Code of Banking Practice (Code des pratiques bancaires) s'appliquent aux banques et aux mutuelles d'épargne et de construction.

	impliquées. Programme d'ombudsman volontaire pour les banques et obligatoire pour les mutuelles d'épargne et de construction.	
Suède	L'office de garantie des dépôts a pris la position que le régime de garantie des dépôts s'applique aux cartes prépayées existantes émises par les banques.	Les lois générales sur la protection des renseignements personnels sont applicables aux banques et aux autres établissements de crédit.
Suisse	Les banques qui participent à des systèmes de monnaie électronique ont développé un plan de partage des pertes en cas d'insolvabilité de l'un des membres du groupe.	Application générale du Code civil.

Recommandations révisées du GAFI

Introduction

1. Le Groupe d'action financière sur le blanchiment de capitaux (GAFI) est un organisme intergouvernemental qui a pour objectif de concevoir et de promouvoir des stratégies de lutte contre le blanchiment de capitaux, processus consistant à dissimuler l'origine illégale des produits de nature criminelle. Ces stratégies visent à empêcher que ces produits soient utilisés dans le cadre d'activités criminelles futures et qu'ils nuisent aux activités économiques légitimes.

2. Le GAFI regroupe actuellement 26 pays (Dans le présent document, la mention du mot « pays » vise également les « territoires » ou « juridictions ».) Les vingt-six pays et gouvernements membres du GAFI sont : l'Allemagne, l'Australie, l'Autriche, la Belgique, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, Hong Kong, l'Irlande, l'Islande, l'Italie, le Japon, le Luxembourg, la Norvège, la Nouvelle-Zélande, le Portugal, le Royaume des Pays-Bas, le Royaume-Uni, Singapour, la Suède, la Suisse et la Turquie) et deux organisations internationales. Les deux organisations internationales sont la Commission européenne et le Conseil de coopération du Golfe. Il compte parmi ses membres les principaux centres financiers d'Europe, d'Amérique du Nord et d'Asie. Il s'agit d'un organisme multidisciplinaire — condition fondamentale pour lutter contre le blanchiment — qui concentre en son sein les pouvoirs de décision d'experts en ce qui concerne les questions juridiques et financières et l'application de la loi.

3. Cette nécessité de couvrir tous les aspects de la lutte contre le blanchiment de capitaux se reflète dans la portée des quarante Recommandations du GAFI, mesures que le Groupe d'action est convenu de mettre en oeuvre et que tous les pays sont encouragés à adopter. Ces quarante Recommandations, rédigées à l'origine en 1990, ont été révisées en 1996 pour prendre en compte l'expérience des six précédentes années et pour refléter l'évolution intervenue sur la question du blanchiment de capitaux. (De 1990 à 1995, le GAFI a aussi élaboré diverses notes interprétatives dont l'objet est de clarifier l'application de recommandations spécifiques. Certaines de ces notes interprétatives ont été actualisées dans le cadre de l'exercice d'inventaire pour refléter les changements dans les recommandations.)

4. Les quarante Recommandations constituent le fondement des efforts de lutte contre le blanchiment de capitaux et elles ont été conçues pour une application universelle. Elles portent sur le système de justice pénale et l'application des lois, le système financier et sa réglementation, ainsi que sur la coopération internationale.

5. Le GAFI a reconnu dès le départ que les pays étaient dotés de systèmes juridiques et financiers divers et que, en conséquence, ils ne pouvaient pas tous prendre des mesures identiques. Les Recommandations constituent donc les principes d'action dans le domaine du

blanchiment que les pays doivent mettre en oeuvre en fonction de leurs circonstances particulières et de leurs cadres constitutionnels; elles leur laissent une marge de manoeuvre plutôt que de tout leur imposer dans le détail. Les mesures ne sont pas particulièrement complexes ou difficiles, mais il doit y avoir une volonté politique d'agir. Elles ne risquent pas non plus de compromettre la liberté d'effectuer des opérations légitimes ou de menacer le développement économique.

6. Les pays du GAFI se sont clairement engagés à accepter la discipline qui consiste à se soumettre à une surveillance multilatérale et à des examens mutuels. Pour tous les pays membres, la mise en oeuvre des quarante Recommandations est supervisée selon une approche en deux volets : un exercice annuel d'auto-évaluation et une procédure plus détaillée d'évaluation mutuelle dans le cadre de laquelle chaque membre fait l'objet d'un examen sur place. Par ailleurs, le GAFI effectue des examens horizontaux des mesures prises pour mettre en oeuvre certaines recommandations particulières.

7. Ces mesures sont essentielles à la création d'un cadre efficace de lutte contre le blanchiment de capitaux.

QUARANTE RECOMMANDATIONS DU GROUPE DE TRAVAIL

A. CADRE GÉNÉRAL DES RECOMMANDATIONS

1. Chaque pays devrait prendre des mesures immédiates pour ratifier et mettre en oeuvre sans restrictions la Convention des Nations-Unies sur le trafic illicite des stupéfiants et des substances psychotropes (Convention de Vienne).

2. Les lois sur le secret professionnel des institutions financières devraient être conçues de telle façon qu'elles n'entravent pas la mise en oeuvre des Recommandations.

3. Un programme efficace de lutte contre le blanchiment d'argent devrait comprendre une amélioration de la coopération multilatérale et de l'entraide judiciaire dans les enquêtes et les poursuites pour des cas de blanchiment de capitaux, ainsi que des procédures d'extradition lorsque c'est possible.

B. RÔLE DES SYSTÈMES JURIDIQUES NATIONAUX DANS LA LUTTE CONTRE LE BLANCHIMENT DE CAPITAUX

Champ d'application de l'infraction de blanchiment de capitaux

4. Chaque pays devrait prendre les mesures nécessaires, y compris des mesures législatives, en vue de criminaliser le blanchiment des fonds comme le prévoit la Convention de Vienne. Chaque pays devrait étendre l'infraction du blanchiment des capitaux issus du trafic de stupéfiants au blanchiment de capitaux se rapportant aux infractions graves. Chaque pays déterminerait quelles infractions graves doivent être considérées comme des infractions sous-jacentes du blanchiment de capitaux.

5. Comme le prévoit la Convention de Vienne, l'infraction de blanchiment de capitaux devrait s'appliquer au moins aux activités intentionnelles de blanchiment, étant entendu que l'élément intentionnel peut être déduit de circonstances factuelles objectives.

6. Dans la mesure du possible, les sociétés elles-mêmes, et non pas seulement leurs employés, devraient être assujetties à la responsabilité pénale.

Mesures provisoires et confiscation

7. Les pays devraient, au besoin, adopter des mesures similaires à celles qui sont indiquées dans la Convention de Vienne, y compris des mesures législatives, afin que leurs autorités compétentes soient en mesure de confisquer les biens blanchis, les produits en découlant, ainsi que les instruments utilisés ou devant l'être pour commettre toute infraction de blanchiment, ou encore des biens de valeur correspondante, sans préjudice des droits des tiers de bonne foi.

De telles mesures devraient permettre : 1) d'identifier, de retrouver et d'évaluer les biens faisant l'objet d'une mesure de confiscation; 2) de mettre en oeuvre des mesures provisoires, tels le gel et la saisie, afin de faire obstacle à toute transaction, tout transfert ou toute cession de tels biens, et 3) de prendre les mesures d'enquête appropriées.

Outre la confiscation et les sanctions pénales, certains pays devraient aussi envisager des sanctions pécuniaires et civiles ou des poursuites judiciaires, notamment devant une juridiction civile, afin d'annuler les contrats conclus lorsque les parties savaient ou auraient dû savoir que le contrat préjudicierait à la faculté pour ce pays de recouvrer ses créances, par exemple, par le biais d'une confiscation ou en infligeant des amendes et autres peines.

C. RÔLE DU SYSTÈME FINANCIER DANS LA LUTTE CONTRE LE BLANCHIMENT DE CAPITAUX

8. Les recommandations 10 à 29 devraient s'appliquer non seulement aux banques mais également aux institutions financières non bancaires. Même pour les institutions financières non bancaires qui ne sont pas soumises à un régime de surveillance prudentielle formelle dans tous les pays, par exemple les bureaux de change, les gouvernements devraient s'assurer que ces institutions sont assujetties aux mêmes lois et règlements anti-blanchiment que toutes les autres institutions financières, et que ces lois et règlements sont appliqués effectivement.

9. Les autorités nationales concernées devraient envisager d'appliquer les recommandations 10 à 21 et 23 à l'exercice d'activités financières, à but commercial, par des entreprises ou professions qui ne sont pas des institutions financières, lorsqu'un tel exercice est autorisé ou non interdit. Les « activités financières » comprennent, de manière non limitative, les activités énumérées dans l'annexe ci-jointe. Il appartient à chaque pays de décider si certaines situations ne donneront pas lieu à l'application de mesures anti-blanchiment, par exemple lorsqu'il s'agit d'une activité financière occasionnelle ou limitée.

Règles d'identification des clients et de conservation des documents

10. Les institutions financières ne devraient pas tenir de comptes anonymes ni de comptes sous des noms manifestement fictifs; elles devraient être tenues (par des lois, des règlements, des accords entre autorités de contrôle et institutions financières, ou par des accords d'autodiscipline entre institutions financières) d'identifier, sur la base d'un document officiel ou d'une autre pièce d'identité fiable, leurs clients habituels ou occasionnels, et d'enregistrer cette identité, lorsqu'elles nouent des relations d'affaires ou effectuent des transactions (en particulier lorsqu'elles ouvrent des comptes ou des livrets, lorsqu'elles réalisent des transactions fiduciaires, lorsqu'elles louent des coffres, lorsqu'elles procèdent à des transactions importantes en espèces).

Afin de satisfaire aux exigences d'identification concernant les personnes morales, les institutions financières devraient, si nécessaire, prendre des mesures telles que :

(i) vérifier l'existence et la structure juridiques du client en obtenant de celui-ci ou d'un registre public, ou de ces deux sources, une preuve de la constitution en personne morale, y compris des renseignements sur le nom du client, sa forme juridique, son adresse, ses dirigeants et les dispositions régissant le pouvoir d'engager la personne morale;

(ii) vérifier que toute personne prétendant agir au nom du client est autorisée à le faire et identifier cette personne.

11. Les institutions financières devraient prendre des mesures raisonnables pour obtenir des renseignements sur l'identité véritable des personnes dans l'intérêt desquelles un compte est ouvert ou une transaction est effectuée, s'il y a le moindre doute sur le fait que ces clients pourraient ne pas agir pour leur propre compte, par exemple dans le cas de sociétés de domicile (c'est-à-dire des institutions, des sociétés, des fondations, des fiducies, etc., qui ne se livrent pas à des opérations commerciales ou industrielles ni à aucune autre forme d'activité commerciale dans le pays où est situé leur siège social).

12. Les institutions financières devraient conserver pendant au moins cinq ans tous les dossiers nécessaires se rapportant aux transactions effectuées, à la fois nationales et internationales, afin de pouvoir répondre rapidement aux demandes d'information des autorités compétentes. Ces dossiers doivent être suffisamment complets pour permettre de reconstituer les transactions individuelles (y compris les montants et les types d'espèces en cause, s'il y en a) de façon à fournir, si nécessaire, des preuves en cas de poursuites pour conduite criminelle.

Les institutions financières devraient tenir des registres concernant l'identité de leurs clients (par exemple, copie ou enregistrement de pièces d'identité officielles comme les passeports, les cartes d'identité, les permis de conduire, ou de documents similaires), les livres de comptes et la correspondance commerciale pendant cinq ans au moins après la clôture du compte.

Ces documents devraient être à la disposition des autorités nationales compétentes, dans le cadre de leurs poursuites et de leurs enquêtes pénales.

13. Les pays devraient apporter une attention particulière aux menaces de blanchiment de capitaux qui découlent des technologies nouvelles ou en développement, lesquelles risquent de favoriser l'anonymat, et prendre des mesures supplémentaires, si nécessaire, pour éviter l'utilisation de ces technologies dans les dispositifs de blanchiment de capitaux.

Diligence accrue des institutions financières

14. Les institutions financières devraient apporter une attention particulière à toutes les opérations importantes, complexes et inhabituelles et à tous les types inhabituels de transactions, lorsqu'elles n'ont pas de but économique ou licite apparent. Le contexte et l'objet de telles opérations devraient être examinés dès que possible; les résultats de cet examen devraient être établis par écrit, et être disponibles pour aider les superviseurs, les vérificateurs et les autorités chargées de l'application des lois.

15. Lorsque les institutions financières suspectent que des fonds proviennent d'une activité criminelle, elles devraient être obligées à déclarer rapidement leurs soupçons aux autorités compétentes.

16. Les institutions financières, leurs dirigeants et leurs employés devraient être protégés par des dispositions législatives contre toute responsabilité, pénale ou civile, pour violation des règles de confidentialité - qu'elles soient imposées par contrat ou par toute disposition législative, réglementaire ou administrative - s'ils déclarent de bonne foi leurs soupçons aux autorités compétentes, même s'ils ne savent pas précisément quelle était l'activité criminelle en question, et même si l'activité illégale soupçonnée ne s'est pas produite.

17. Les institutions financières, leurs dirigeants et leurs employés ne devraient pas avertir leurs clients ou, le cas échéant, ne devraient pas être autorisés à les avertir, lorsqu'ils portent à la connaissance des autorités compétentes des renseignements relatifs à ces clients.

18. Les institutions financières qui déclarent leurs soupçons devraient se conformer aux instructions provenant des autorités compétentes.

19. Les institutions financières devraient mettre au point des programmes de lutte contre le blanchiment de capitaux; ces programmes devraient comprendre au minimum :

(i) des politiques, des procédures et des contrôles internes, y compris la désignation de personnes responsables au niveau de la direction générale, et des procédures de sélection adéquates lors de l'embauche des employés, de façon à s'assurer qu'elle s'effectue selon des critères exigeants;

(ii) un programme continu de formation des employés;

(iii) une fonction de vérification pour contrôler l'efficacité du système.

Mesures pour faire face au problème des pays dépourvus totalement ou partiellement de dispositifs de lutte contre le blanchiment de capitaux

20. Les institutions financières devraient s'assurer que les principes susmentionnés sont également appliqués par leurs succursales et leurs filiales majoritaires situées à l'étranger, particulièrement dans les pays qui n'appliquent pas ou qui appliquent trop peu ces recommandations, dans la mesure où les lois et les règlements locaux le permettent. Lorsque les mêmes lois et règlements s'y opposent, les institutions financières devraient informer les autorités compétentes du pays où est située la société mère qu'elles ne peuvent pas appliquer ces recommandations.

21. Les institutions financières devraient porter une attention particulière à leurs relations d'affaires et à leurs transactions avec les personnes physiques et morales, y compris les compagnies et les institutions financières, résidant dans les pays qui n'appliquent pas ou qui appliquent peu les présentes recommandations. Lorsque ces transactions n'ont pas d'objet économique ou licite apparent, leur contexte et leur objet devraient être examinés dans la mesure du possible; les résultats de cet examen devraient être établis par écrit et être disponibles pour aider les superviseurs, les vérificateurs et les autorités chargées de l'application des lois.

Autres mesures pour éviter le blanchiment des capitaux

22. Les pays devraient songer à la mise en oeuvre de mesures réalistes destinées à détecter ou à surveiller la circulation physique transfrontalière d'espèces et d'instruments au porteur, à la condition que cette information soit utilisée à bon escient et que la liberté des mouvements de capitaux ne se trouve en aucune façon entravée.

23. Les pays devraient réfléchir à la faisabilité et à l'utilité d'un système dans lequel les banques et d'autres institutions financières et intermédiaires déclareraient toutes les transactions nationales et internationales en espèces au-dessus d'un certain montant à une agence centrale nationale disposant d'une base de données informatisée; cette information serait accessible aux autorités compétentes dans les affaires de blanchiment de capitaux et son utilisation serait strictement limitée.

24. Les pays devraient davantage encourager, de façon générale, la mise en oeuvre de techniques modernes et sûres de gestion de fonds. Un usage accru des chèques, des cartes de débit, des virements automatiques de salaires et de l'enregistrement automatisé des opérations sur titres serait un moyen d'encourager la réduction des transferts d'espèces.

25. Les pays devraient prêter attention aux possibilités d'utilisation abusive de personnes morales inactives par les auteurs d'opérations de blanchiment de capitaux; ils devraient envisager de prendre des mesures supplémentaires pour prévenir une utilisation illicite de ces entités.

Mise en oeuvre des recommandations et rôle des autorités de réglementation et d'autres autorités administratives

26. Les autorités compétentes chargées du contrôle des banques et d'autres institutions financières ou intermédiaires et les autres autorités compétentes devraient s'assurer que les institutions contrôlées disposent de programmes adéquats pour éviter le blanchiment de capitaux. Ces autorités devraient coopérer avec les autorités nationales judiciaires ou avec les autorités chargées de l'application des lois et leur apporter leur concours, soit spontanément, soit sur demande, dans les enquêtes et les poursuites relatives au blanchiment de capitaux.

27. Des autorités administratives compétentes devraient être désignées pour assurer la mise en oeuvre effective de l'ensemble des présentes recommandations par un contrôle et une réglementation des professions non bancaires recevant des espèces, telles que définies par chaque pays.

28. Les autorités compétentes devraient établir des directives pour aider les institutions financières à détecter des modes de comportement suspects chez leurs clients. Il est clair que de telles directives devront évoluer dans le temps et qu'elles n'auront jamais un caractère exhaustif. De plus, elles seront surtout utilisées pour former le personnel des institutions financières.

29. Les autorités compétentes qui assurent la réglementation ou la supervision des institutions financières devraient prendre les mesures législatives ou réglementaires nécessaires pour éviter que des criminels ou leurs complices ne prennent le contrôle d'institutions financières ou n'y acquièrent une participation significative.

RENFORCEMENT DE LA COOPÉRATION INTERNATIONALE

Coopération administrative / Échange d'information de caractère général

30. Les administrations nationales devraient envisager d'enregistrer, au moins sous forme agrégée, les flux internationaux d'espèces en toutes devises, pour rendre possible, en combinant ces données avec celles émanant d'autres sources étrangères et avec les informations détenues par les banques centrales, des estimations des flux d'espèces entre pays. Ces informations devraient être mises à la disposition du Fonds monétaire international et de la Banque des règlements internationaux pour faciliter les études internationales.

31. Les autorités internationales compétentes, peut-être l'Interpol et l'Organisation mondiale des douanes, devraient être chargées de rassembler puis de diffuser aux autorités compétentes les informations relatives aux évolutions les plus récentes en matière de blanchiment de capitaux et de techniques de blanchiment. Les banques centrales et les organes de réglementation bancaire pourraient également le faire dans le secteur dont ils ont la charge. Les autorités nationales des différents secteurs, en consultation avec des associations professionnelles, pourraient alors diffuser ces renseignements auprès d'institutions financières dans chaque pays.

Échange d'information relative à des transactions suspectes

32. Chaque pays devrait s'efforcer d'améliorer un échange international d'information spontané ou « sur commande » entre autorités compétentes, relatif à des opérations suspectes, et à des personnes ou des sociétés impliquées dans ces opérations. Des garanties strictes devraient être instituées pour assurer la conformité de cet échange d'information avec les dispositions nationales et internationales en matière de protection de la vie privée et de sécurité des données.

Autres formes de coopération

Fondements de la coopération en matière de confiscation, d'entraide judiciaire et d'extradition, et moyens à prendre à ce sens

33. Les pays devraient essayer de veiller, dans un cadre bilatéral ou multilatéral, à ce que les différents critères pris en compte dans les définitions nationales au titre de la connaissance de l'acte commis - c'est-à-dire les différents critères relatifs à l'élément intentionnel de l'infraction - n'affectent pas la capacité ou la volonté des pays de se prêter mutuellement assistance en matière judiciaire.

34. La coopération internationale devrait s'appuyer sur un réseau d'accords et d'arrangements bilatéraux et multilatéraux fondés sur des concepts juridiques communs, destinés à mettre en oeuvre des mesures pratiques au bénéfice d'une entraide mutuelle aussi large que possible.

35. Les pays devraient être encouragés à ratifier et mettre en oeuvre les conventions internationales pertinentes sur le blanchiment d'argent, telles que la Convention de 1990 du Conseil de l'Europe sur le blanchiment de capitaux, la perquisition, la fouille, la saisie et la confiscation des produits d'activités criminelles.

Orientations pour l'amélioration de l'entraide judiciaire dans le domaine du blanchiment d'argent

36. La coopération entre les autorités compétentes appropriées des différents pays devrait être encouragée dans le cadre des enquêtes. À cet égard, une technique d'enquête valable et efficace est la livraison surveillée relative aux actifs connus comme étant des produits du crime ou suspectés en être. Les pays sont encouragés à soutenir cette technique, lorsque cela est possible.

37. Il conviendrait de prévoir des procédures d'entraide judiciaire en matière pénale concernant le recours à des mesures de contrainte telles que la production de documents par des institutions financières et d'autres personnes, la fouille de personnes et de locaux, la saisie et l'obtention d'éléments de preuve destinés à être utilisés dans des enquêtes et des poursuites en matière de blanchiment et dans des procédures connexes devant des juridictions étrangères.

38. Il serait souhaitable que l'on puisse prendre des mesures rapides en réponse à des requêtes émanant de gouvernements étrangers demandant d'identifier, de geler, de saisir et de confisquer les produits, ou d'autres biens d'une valeur équivalente à ces produits, tirés du blanchiment d'argent ou des délits sur lesquels repose l'activité de blanchiment.

39. Afin d'éviter les conflits de compétence, il conviendrait d'étudier la possibilité d'élaborer et de mettre en oeuvre des mécanismes permettant de déterminer, dans l'intérêt de la justice, le ressort le plus approprié pour le jugement des défendeurs, dans des affaires qui pourraient faire l'objet de poursuites dans plusieurs pays. De même, il devrait exister des mesures visant à coordonner les procédures de saisie et de confiscation et pouvant inclure le partage des avoirs confisqués.

40. Les pays devraient mettre en place des procédures permettant d'extrader, lorsque cela est possible, des individus accusés de blanchiment de capitaux ou d'infractions connexes. Dans le respect de son système juridique national, chaque pays devrait reconnaître le blanchiment de capitaux comme une infraction pouvant donner lieu à extradition. Dans la mesure où leurs structures juridiques le permettent, les pays pourraient envisager de simplifier l'extradition, par la transmission directe des demandes d'extradition entre les ministères appropriés, l'extradition des personnes sur le seul fondement de mandats d'arrêt ou de jugements, l'extradition de leurs ressortissants nationaux ou l'extradition simplifiée de personnes acceptant de renoncer à la procédure formelle d'extradition.

Annexe à la Recommandation 9 : Liste des activités financières entreprises par des professions ou institutions qui ne sont pas des institutions financières

1. Acceptation de dépôts et d'autres fonds remboursables du public.

2. Prêts (y compris : le crédit à la consommation, le crédit hypothécaire, l'affacturage avec ou sans recours, le financement de transactions commerciales (forfaitage inclus).

3. Crédit-bail.

4. Services de transmission monétaire.

5. Émission et gestion de moyens de paiement (par exemple, cartes de crédit et de débit, chèques, chèques de voyage et traites bancaires, etc.).

6. Octroi de garanties et souscription d'engagements.

7. Négociation pour le compte de clients (marché au comptant, marché à terme, swaps, opérations à terme, options...) en ce qui concerne :

    a) les instruments du marché monétaire (chèques, effets, certificats de dépôt, etc.);

b) le marché des changes;

c) les instruments sur devises, taux d'intérêt et indices;

d) les valeurs mobilières cessibles;

e) les marchés à terme de marchandises.

8. Participation à des émissions de valeurs mobilières et prestation de services financiers connexes.

9. Gestion individuelle et collective du patrimoine.

10. Conservation et administration des titres garantis par des fonds pour le compte des clients.

11. Assurance sur la vie et autres produits de placement dans le domaine de l'assurance.

12. Le change manuel.